(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－164879
（P2002－164879A）
(43)公開日　平成14年６月７日(2002.6.7)

(51)Int.Cl.'		識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ	9/08		Ｇ０６Ｆ	13/00	５４０Ｓ　５Ｄ０４４
Ｇ０６Ｆ	13/00	５４０		17/60	１４２　５Ｊ１０４
	17/60	１４２			３０２Ｅ
		３０２	Ｇ０９Ｃ	5/00	
Ｇ０９Ｃ	5/00		Ｇ１０Ｋ	15/02	

審査請求　未請求　請求項の数20　ＯＬ　（全 71 頁）　最終頁に続く

(21)出願番号　特願2000－361631(P2000－361631)

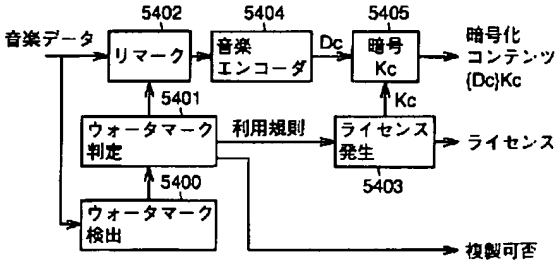
(22)出願日　平成12年11月28日(2000.11.28)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(71)出願人　000136136
株式会社ピーエフユー
石川県河北郡宇ノ気町字宇野気ヌ98番地の２
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

最終頁に続く

(54)【発明の名称】　データ端末装置

(57)【要約】
【課題】　コンテンツデータの利用規則性に応じてコンテンツデータをリッピングできるデータ端末装置を提供する。
【解決手段】　ウォーターマーク検出手段５４００は、音楽データからウォーターマークを検出し、ウォーターマーク判定手段５４０１は、検出したウォーターマークの利用規則に規則性が有るか否かを判定する。そして、ライセンス発生手段５４０３は、ウォーターマークの利用規則の規則性に応じてライセンスを発生する。リマーク手段５４０２は、ウォーターマークの利用規則の規則性に応じて音楽データの複製条件を変更したウォーターマークを付け替える。音楽エンコーダ５４０４は、リマーク手段５４０２からの音楽データを所定の方式に符号化する。暗号手段５４０５は、音楽エンコーダ５４０４からの音楽データをライセンス発生手段５４０３により発生されたライセンス鍵によって暗号化する。



【特許請求の範囲】
【請求項１】　平文のコンテンツデータを取得し、前記コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータを復号して再生するためのローカルライセンスとを生成するデータ端末装置であって、
前記コンテンツデータに含まれる複製可否情報に基づいて前記ローカルライセンスを生成し、その生成したローカルライセンスに含まれるライセンス鍵によって前記コンテンツデータを暗号化して前記暗号化コンテンツデータを生成する暗号化コンテンツ生成手段と、
前記生成したローカルライセンスに独自の暗号化を施した暗号化ローカルライセンスを生成する暗号処理手段と、
前記暗号化ローカルライセンスおよび暗号化コンテンツデータを記憶する記憶手段と、
制御部とを備え、
前記制御部は、前記取得したコンテンツデータを前記暗号化コンテンツ生成手段へ与え、前記ローカルライセンスを前記暗号処理手段へ与える、データ端末装置。
【請求項２】　コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータを復号して再生するためのライセンスとを配信サーバから受信し、および／または前記コンテンツデータを取得して前記暗号化コンテンツデータと前記暗号化コンテンツデータを復号して再生するためのローカルライセンスとを生成するデータ端末装置であって、
前記配信サーバとの間で相互認証を行って前記暗号化コンテンツデータおよび前記ライセンスを前記配信サーバから受信し、かつ、前記ライセンスを保持するライセンス管理デバイスと、
前記コンテンツデータに含まれる複製可否情報に基づいて前記ローカルライセンスを生成し、その生成したローカルライセンスに含まれるライセンス鍵によって前記コンテンツデータを暗号化して前記暗号化コンテンツデータを生成する暗号化コンテンツ生成手段と、
前記生成したローカルライセンスに独自の暗号化を施した暗号化ローカルライセンスを生成する暗号処理手段と、
前記ライセンス、前記暗号化ローカルライセンスおよび前記暗号化コンテンツデータを記憶する記憶手段と、
制御部とを備え、
前記制御部は、前記取得したコンテンツデータを前記暗号化コンテンツ生成手段へ与え、前記ローカルライセンスを前記暗号処理手段へ与える、データ端末装置。
【請求項３】　コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータを復号して再生するためのライセンスとを配信サーバから受信し、および／または前記コンテンツデータを取得して前記暗号化コンテンツデータと前記暗号化コンテンツデータを復号して再生するためのローカルライセンスとを生成するデータ端末装置であって、
ソフトウエアによって、前記配信サーバとの間で相互認証を行い、かつ、前記暗号化コンテンツデータおよび前記ライセンスを前記配信サーバから受信するライセンス管理モジュールと、
前記コンテンツデータに含まれる複製可否情報に基づいて前記ローカルライセンスを生成し、その生成したローカルライセンスに含まれるライセンス鍵によって前記コンテンツデータを暗号化して前記暗号化コンテンツデータを生成する暗号化コンテンツ生成手段と、
前記生成したローカルライセンスに独自の暗号化を施した暗号化ローカルライセンス、または前記受信したライセンスに独自の暗号化を施した暗号化ライセンスを生成する暗号処理手段と、
前記暗号化ライセンス、前記暗号化ローカルライセンスおよび前記暗号化コンテンツデータを記憶する記憶手段と、
制御部とを備え、
前記制御部は、前記取得したコンテンツデータを前記暗号化コンテンツ生成手段へ与え、前記ローカルライセンスおよび前記ライセンスを前記暗号処理手段へ与える、データ端末装置。
【請求項４】　コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータを復号して再生するためのライセンスとを配信サーバから受信し、および／または前記コンテンツデータを取得して前記暗号化コンテンツデータと前記暗号化コンテンツデータを復号して再生するためのローカルライセンスとを生成するデータ端末装置であって、
前記配信サーバとの間で相互認証を行って前記暗号化コンテンツデータおよび前記ライセンスを前記配信サーバから受信し、かつ、前記ライセンスを保持するライセンス管理デバイスと、
ソフトウエアによって、前記配信サーバとの間で相互認証を行い、かつ、前記暗号化コンテンツデータおよび前記ライセンスを前記配信サーバから受信するライセンス管理モジュールと、
前記コンテンツデータに含まれる複製可否情報に基づいて前記ローカルライセンスを生成し、その生成したローカルライセンスに含まれるライセンス鍵によって前記コンテンツデータを暗号化して前記暗号化コンテンツデータを生成する暗号化コンテンツ生成手段と、
前記生成したローカルライセンスに独自の暗号化を施した暗号化ローカルライセンス、または前記ライセンス管理モジュールによって受信されたライセンスに独自の暗号化を施した暗号化ライセンスを生成する暗号処理手段と、
前記暗号化ライセンス、前記暗号化ローカルライセンスおよび前記暗号化コンテンツデータを記憶する記憶手段

と、
制御部とを備え、
前記制御部は、前記取得したコンテンツデータを前記暗号化コンテンツ生成手段へ与え、前記ライセンスおよび前記ローカルライセンスを前記暗号処理手段へ与える、データ端末装置。
【請求項５】　前記暗号化コンテンツ生成手段は、前記生成した暗号化コンテンツデータおよびローカルライセンスを他の装置へ貸出すための貸出可能数をさらに生成し、
前記暗号処理手段は、前記ローカルライセンスと前記貸出可能数とに独自の暗号化を施し、前記暗号化ローカルライセンスを生成する、請求項１から請求項４のいずれか１項に記載のデータ端末装置。
【請求項６】　前記暗号化ローカルライセンスを少なくとも含むライセンス管理ファイルを生成するファイル生成手段をさらに備え、
前記制御部は、前記暗号化コンテンツデータおよび前記ライセンス管理ファイルを前記記憶手段に与える、請求項１から請求項５のいずれか１項に記載のデータ端末装置。
【請求項７】　前記暗号化コンテンツ生成手段は、前記複製可否情報が複製を許可する複製許可情報であるとき、前記複製許可情報を反映したローカルライセンスを生成する、請求項１から請求項６のいずれか１項に記載のデータ端末装置。
【請求項８】　前記暗号化コンテンツ生成手段は、
前記複製可否情報が複製を許可する複製許可情報であるとき、前記複製許可情報を反映したローカルライセンスを生成し、
前記コンテンツデータが前記複製可否情報を含まないとき、前記暗号化コンテンツデータを復号して再生するためのライセンスの複製および移動を禁止したローカルライセンスを生成する、請求項１から請求項６のいずれか１項に記載のデータ端末装置。
【請求項９】　前記コンテンツデータを記録した記録媒体を駆動する媒体駆動手段をさらに備え、
前記制御部は、前記媒体駆動手段が前記記録媒体から読出したコンテンツデータを前記暗号化コンテンツ生成手段へ与える、請求項１から請求項８のいずれか１項に記載のデータ端末装置。
【請求項１０】　前記制御部は、インターネットによって受信したコンテンツデータを前記暗号化コンテンツ生成手段に与える、請求項１から請求項８のいずれか１項に記載のデータ端末装置。
【請求項１１】　前記暗号化コンテンツ生成手段は、
前記複製可否情報を前記コンテンツデータから検出する複製可否情報検出手段と、
前記検出した複製可否情報を判定する複製可否情報判定手段と、
前記複製可否情報判定手段の判定結果に基づいて前記ローカルライセンスを生成するライセンス生成手段と、
前記ライセンス鍵によって前記コンテンツデータを暗号化する暗号手段とを含む、請求項１から請求項１０のいずれか１項に記載のデータ端末装置。
【請求項１２】　前記暗号化コンテンツ生成手段は、
前記複製可否情報を前記コンテンツデータから検出する複製可否情報検出手段と、
前記検出した複製可否情報を判定する複製可否情報判定手段と、
前記複製可否情報判定手段の判定結果に基づいて複製条件を変更して前記コンテンツデータに書込む複製条件変更手段と、
前記複製条件変更手段からのコンテンツデータを所定の方式に符号化する符号化手段と、
前記複製可否情報判定手段の判定結果に基づいて前記ローカルライセンスを生成するライセンス生成手段と、
前記所定の方式に符号化されたコンテンツデータを前記ライセンス鍵によって暗号化する暗号手段とを含む、請求項１から請求項１０のいずれか１項に記載のデータ端末装置。
【請求項１３】　前記ライセンス生成手段は、前記暗号化コンテンツデータを特定するコンテンツ識別子と、前記暗号化コンテンツデータおよび前記ライセンスを他の装置へ貸出すときの通信を特定する通信識別子と、前記ライセンス鍵と、前記暗号化コンテンツデータおよび前記ローカルライセンスを記録するデータ記録装置に対する記録装置アクセス条件と、前記ライセンスによって前記暗号化コンテンツデータを復号して再生するデータ再生装置に対する再生装置アクセス条件とから成る前記ローカルライセンスを生成する、請求項１２に記載のデータ端末装置。
【請求項１４】　前記コンテンツ識別子および前記通信識別子は、固定領域と、前記固定領域に続く管理領域とから成り、
前記ライセンス生成手段は、前記コンテンツ識別子または前記通信識別子がデータ端末装置において生成されたことを示すローカル信号を前記固定領域に書込み、前記暗号化コンテンツデータに対応する識別番号を前記管理領域に書込んでコンテンツ識別子および通信識別子を生成する、請求項１３に記載のデータ端末装置。
【請求項１５】　前記ライセンス生成手段は、前記通信識別子と前記ライセンス鍵とを乱数の発生によって生成する、請求項１３に記載のデータ端末装置。
【請求項１６】　前記記録装置アクセス条件は、
前記暗号化コンテンツデータの再生の可否および可能回数を表す再生可能回数と、
前記暗号化コンテンツデータおよびローカルライセンスの移動および複製を制御する移動複製制御情報と、
前記ローカルライセンスの保護レベルを表す保護レベル

情報とから成る、請求項１３に記載のデータ端末装置。
【請求項１７】　前記再生可能回数は、前記暗号化コンテンツデータの再生不可を表す固定値から成る第１の再生可能回数と、前記暗号化コンテンツデータの再生を許諾する毎に単調減少する変動値から成る第２の再生可能回数と、前記暗号化コンテンツデータの再生を無制限に許諾する第３の再生可能回数とから成り、
前記移動複製制御情報は、
前記暗号化コンテンツデータおよび前記ローカルライセンスの移動および複製を禁止する第１の制御情報と、
前記暗号化コンテンツデータおよび前記ローカルライセンスの移動を禁止し、前記暗号化コンテンツデータおよび前記ローカルライセンスの複製を条件付きで許諾する第２の制御情報と、
前記暗号化コンテンツデータおよび前記ローカルライセンスの移動および複製を条件付きで許諾する第３の制御情報と、
前記暗号化コンテンツデータおよび前記ローカルライセンスの移動を許可し、前記暗号化コンテンツデータおよび前記ローカルライセンスの複製を禁止する第４の制御情報と、
前記暗号化コンテンツデータおよび前記ローカルライセンスの移動および複製を無制限に許諾する第５の制御情報とから成る、請求項１６に記載のデータ端末装置。
【請求項１８】　前記第２の制御情報は、前記暗号化コンテンツデータおよび前記ローカルライセンスの複製毎に単調減少し、かつ、複製可能回数を表す変動値を含み、
前記第３の制御情報は、前記暗号化コンテンツデータおよび前記ローカルライセンスの移動および複製毎に単調増加する変動値を含む、請求項１７に記載のデータ端末装置。
【請求項１９】　前記再生装置アクセス条件は、
前記暗号化コンテンツデータの再生速度の変換可否を示す第１の信号と、
前記暗号化コンテンツデータの編集の可否を示す第２の信号と、
再生可能な暗号化コンテンツデータのサイズを示す第３の信号と、
前記暗号化コンテンツデータの利用最終日時を示す第４の信号と、
前記暗号化コンテンツデータの利用開始日時を示す第５の信号と、
地域コードとから成る、請求項１３に記載のデータ端末装置。
【請求項２０】　前記貸出情報は、
前記暗号化コンテンツデータおよび前記ローカルライセンスの貸出しを禁止する禁止情報と、
前記暗号化コンテンツデータおよび前記ローカルライセンスの貸出し毎に単調減少し、前記暗号化コンテンツデータおよび前記ローカルライセンスの返却毎に単調増加する貸出許可情報とから成る、請求項１３に記載のデータ端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ端末装置に関するものである。
【０００２】
【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。
【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。
【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。
【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。
【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。
【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。
【０００８】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受

ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００９】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【００１２】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【００１３】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【００１４】一方、インターネットを用いて暗号化コンテンツデータをパーソナルコンピュータに配信することも行なわれている。そして、パーソナルコンピュータへの暗号化コンテンツデータの配信においては、パーソナルコンピュータにインストールされたソフトウエアによって暗号化コンテンツデータの配信が行なわれており、暗号化コンテンツデータに対するセキュリティは、暗号化コンテンツデータをメモリカードに書込む場合より低い。また、上記のメモリカードと同じセキュリティを持つデバイスをパーソナルコンピュータに装着すれば、上記の携帯電話機に対する暗号化コンテンツデータの配信と同じ配信をパーソナルコンピュータに対して行なうことが可能である。

【００１５】そうすると、パーソナルコンピュータは、インストールされたソフトウエアと、上記デバイスとによって暗号化コンテンツデータを受信する。つまり、パーソナルコンピュータは、セキュリティレベルの異なる暗号化コンテンツデータを受信する。

【００１６】さらに、音楽データが記録された音楽ＣＤが広く普及しており、この音楽ＣＤから音楽データをリッピングによって取得することも行なわれている。そして、このリッピングによって音楽データから暗号化音楽データ（暗号化コンテンツデータ）と、その暗号化音楽データを復号して再生するためのライセンスとが生成される。そして、このリッピングにおいては、コンテンツデータの利用規則を規定するウォーターマークをコンテンツデータから検出し、その検出したウォーターマークの内容に応じて暗号化コンテンツデータおよびライセンスが生成される。

【００１７】

【発明が解決しようとする課題】しかし、現行のウォーターマークは、暗号化コンテンツデータおよびライセンスの生成を全く禁止するか、暗号化コンテンツデータを復号して再生するライセンスの移動および複製を禁止したライセンスを生成することを規定しているに過ぎない。したがって、リッピングによって暗号化コンテンツデータおよびライセンスを取得できたとしても、その暗号化コンテンツデータおよびライセンスを移動したり、複製したりすることはできない。また、今後、コンテンツデータの利用規則性をさらに広く認めたウォーターマークの出現も想定され、現在のリッピングでは、そのようなウォーターマークに適合したリッピングを行なうことができない。

【００１８】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、コンテンツデータの利用規則性に応じてコンテンツデータをリッピングできるデータ端末装置を提供することである。

【００１９】

【課題を解決するための手段および発明の効果】この発明によるデータ端末装置は、平文のコンテンツデータを取得し、コンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータを復号して再生するためのローカルライセンスとを生成するデータ端末装置であって、コンテンツデータに含まれる複製可否情報に基づいてローカルライセンスを生成し、その生成したローカルライセンスに含まれるライセンス鍵によってコンテンツデータを暗号化して暗号化コンテンツデータを生成する暗号化コンテンツ生成手段と、生成したローカルライセンスに独自の暗号化を施した暗号化ローカルライセンスを生成する暗号処理手段と、暗号化ローカルライセンスおよび暗号化コンテンツデータを記憶する記憶手段と、制御部とを備え、制御部は、取得したコンテン

ツデータを暗号化コンテンツ生成手段へ与え、ローカルライセンスを暗号処理手段へ与える。

【００２０】この発明によるデータ端末装置においては、平文のコンテンツデータに含まれる複製可否情報を検出し、その検出した複製可否情報の内容に応じてローカルライセンスが生成される。ローカルライセンスは、コンテンツデータを暗号化するためのライセンス鍵を含む。ローカルライセンスが生成されると、ローカルライセンスに含まれるライセンス鍵によってコンテンツデータを暗号化して暗号化コンテンツデータを生成する。そして、生成されたローカルライセンスは、独自の暗号化が施され、暗号化ローカルライセンスとして暗号化コンテンツデータとともに記憶手段に記憶される。

【００２１】したがって、この発明によれば、平文のコンテンツデータから複製可否情報に応じて暗号化コンテンツデータと、その暗号化コンテンツデータを復号して再生するローカルライセンスとを生成できる。

【００２２】また、この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータを復号して再生するためのライセンスとを配信サーバから受信し、および／またはコンテンツデータを取得して暗号化コンテンツデータと暗号化コンテンツデータを復号して再生するためのローカルライセンスとを生成するデータ端末装置であって、配信サーバとの間で相互認証を行って暗号化コンテンツデータおよびライセンスを配信サーバから受信し、かつ、ライセンスを保持するライセンス管理デバイスと、コンテンツデータに含まれる複製可否情報に基づいてローカルライセンスを生成し、その生成したローカルライセンスに含まれるライセンス鍵によってコンテンツデータを暗号化して暗号化コンテンツデータを生成する暗号化コンテンツ生成手段と、生成したローカルライセンスに独自の暗号化を施した暗号化ローカルライセンスを生成する暗号処理手段と、ライセンス、暗号化ローカルライセンスおよび暗号化コンテンツデータを記憶する記憶手段と、制御部とを備え、制御部は、取得したコンテンツデータを暗号化コンテンツ生成手段へ与え、ローカルライセンスを暗号処理手段へ与える。

【００２３】この発明によるデータ端末装置においては、配信サーバから暗号化コンテンツデータとライセンスとが受信され、ライセンスがハードウエアによって保持されるとともに、平文のコンテンツデータから暗号化コンテンツデータおよびローカルライセンスとが生成され、ローカルライセンスは独自の暗号化が施されソフトウエアによって保持される。

【００２４】したがって、この発明によれば、暗号化コンテンツデータとライセンスとを配信サーバから受信可能なデータ端末装置において、平文のコンテンツデータから複製可否情報に応じて暗号化コンテンツデータおよびローカルライセンスを生成できる。

【００２５】また、この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータを復号して再生するためのライセンスとを配信サーバから受信し、および／またはコンテンツデータを取得して暗号化コンテンツデータと暗号化コンテンツデータを復号して再生するためのローカルライセンスとを生成するデータ端末装置であって、ソフトウエアによって、配信サーバとの間で相互認証を行い、かつ、暗号化コンテンツデータおよびライセンスを配信サーバから受信するライセンス管理モジュールと、コンテンツデータに含まれる複製可否情報に基づいてローカルライセンスを生成し、その生成したローカルライセンスに含まれるライセンス鍵によってコンテンツデータを暗号化して前記暗号化コンテンツデータを生成する暗号化コンテンツ生成手段と、生成したローカルライセンスに独自の暗号化を施した暗号化ローカルライセンス、または受信したライセンスに独自の暗号化を施した暗号化ライセンスを生成する暗号処理手段と、暗号化ライセンス、暗号化ローカルライセンスおよび暗号化コンテンツデータを記憶する記憶手段と、制御部とを備え、制御部は、取得したコンテンツデータを暗号化コンテンツ生成手段へ与え、ローカルライセンスおよびライセンスを暗号処理手段へ与える。

【００２６】この発明によるデータ端末装置においては、ソフトウエアによって、配信サーバから暗号化コンテンツデータとライセンスとが受信され、かつ、ライセンスが保持されるとともに、平文のコンテンツデータから暗号化コンテンツデータおよびローカルライセンスとが生成され、ローカルライセンスは独自の暗号化が施されソフトウエアによって保持される。

【００２７】したがって、この発明によれば、ソフトウエアによって暗号化コンテンツデータとライセンスとを配信サーバから受信可能なデータ端末装置において、平文のコンテンツデータから複製可否情報に応じて暗号化コンテンツデータおよびローカルライセンスを生成できる。

【００２８】また、この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータを復号して再生するためのライセンスとを配信サーバから受信し、および／またはコンテンツデータを取得して暗号化コンテンツデータと暗号化コンテンツデータを復号して再生するためのローカルライセンスとを生成するデータ端末装置であって、配信サーバとの間で相互認証を行って暗号化コンテンツデータおよびライセンスを配信サーバから受信し、かつ、ライセンスを保持するライセンス管理デバイスと、ソフトウエアによって、配信サーバとの間で相互認証を行い、かつ、暗号化コンテンツデータおよびライセンスを配信サーバから受信するライセンス管理モジュールと、コンテンツデータに含まれる複製可否情報に基づい

てローカルライセンスを生成し、その生成したローカルライセンスに含まれるライセンス鍵によってコンテンツデータを暗号化して暗号化コンテンツデータを生成する暗号化コンテンツ生成手段と、生成したローカルライセンスに独自の暗号化を施した暗号化ローカルライセンス、またはライセンス管理モジュールによって受信されたライセンスに独自の暗号化を施した暗号化ライセンスを生成する暗号処理手段と、暗号化ライセンス、暗号化ローカルライセンスおよび暗号化コンテンツデータを記憶する記憶手段と、制御部とを備え、制御部は、取得したコンテンツデータを暗号化コンテンツ生成手段へ与え、ライセンスおよびローカルライセンスを暗号処理手段へ与える。

【００２９】この発明によるデータ端末装置は、３つの方法によって暗号化コンテンツデータおよびライセンスを取得する。１つ目の方法は、配信サーバから暗号化コンテンツデータとライセンスとを受信し、ライセンスをハードウエアによって保持する方法である。２つ目の方法は、ソフトウエアによって暗号化コンテンツデータとライセンスとを受信し、かつ、ライセンスを保持する方法である。そして、３つ目の方法は、平文のコンテンツデータから暗号化コンテンツデータおよびローカルライセンスとを生成し、ローカルライセンスに独自の暗号化を施してソフトウエアによって保持する方法である。

【００３０】したがって、この発明によれば、配信サーバからハードウエアおよびソフトウエアによって暗号化コンテンツデータとライセンスとを受信可能なデータ端末装置において、平文のコンテンツデータから複製可否情報に応じて暗号化コンテンツデータおよびローカルライセンスを生成できる。

【００３１】好ましくは、データ端末装置の暗号化コンテンツ生成手段は、生成した暗号化コンテンツデータおよびローカルライセンスを他の装置へ貸出すための貸出可能数をさらに生成し、暗号処理手段は、ローカルライセンスと貸出可能数とに独自の暗号化を施し、暗号化ローカルライセンスを生成する。

【００３２】データ端末装置においては、平文のコンテンツデータから暗号化コンテンツデータとローカルライセンスとを生成するとき、暗号化コンテンツデータおよびローカルライセンスを他の装置へ貸出すための貸出可能数を生成し、その生成した貸出可能数をローカルライセンスとともに暗号化して管理する。

【００３３】したがって、この発明によれば、平文のコンテンツデータから暗号化コンテンツデータおよびローカルライセンスを生成する、いわゆる、リッピングによって取得した暗号化コンテンツデータおよびローカルライセンスを、暗号化コンテンツデータおよびローカルライセンスが保持されたデータ端末装置から取出すことができる。

【００３４】好ましくは、暗号化ローカルライセンスを少なくとも含むライセンス管理ファイルを生成するファイル生成手段をさらに備え、制御部は、暗号化コンテンツデータおよびライセンス管理ファイルを記憶手段に与える。

【００３５】データ端末装置において生成され、かつ、暗号化された暗号化ローカルライセンスは、ライセンス管理ファイルに記録され、記憶手段に保持される。

【００３６】したがって、この発明においては、生成されたローカルライセンスをファイルに入れソフト的に管理できる。

【００３７】好ましくは、データ端末装置の暗号化コンテンツ生成手段は、複製可否情報が複製を許可する複製許可情報であるとき、複製許可情報を反映したローカルライセンスを生成する。

【００３８】平文のコンテンツデータに含まれる複製可否情報が、たとえば、１０回までの複製を許可するという複製許可情報であるとき、１０回までの複製を許可した複製許可回数を含めてローカルライセンスが生成される。

【００３９】したがって、この発明によれば、コンテンツデータが複製可能なものであれば、複製許可情報に基づいて複製可能な暗号化コンテンツデータおよびローカルライセンスを生成できる。

【００４０】好ましくは、データ端末装置の暗号化コンテンツ生成手段は、複製可否情報が複製を許可する複製許可情報であるとき、複製許可情報を反映したローカルライセンスを生成し、コンテンツデータが複製可否情報を含まないとき、暗号化コンテンツデータを復号して再生するためのライセンスの複製および移動を禁止したローカルライセンスを生成する。

【００４１】平文のコンテンツデータに含まれる複製可否情報がコンテンツデータの複製を許可するものであるとき、その許可内容に応じて暗号化コンテンツデータおよびローカルライセンスの複製を許可するローカルライセンスを生成し、コンテンツデータが複製可否情報を含まないとき、暗号化コンテンツデータおよびライセンスの複製および移動を禁止するローカルライセンスを生成する。つまり、コンテンツデータが複製可否情報を含まない種類のコンテンツデータであるとき、データ端末装置は、複製可否情報に応じてローカルライセンスを生成できないが、リッピングによって生成された暗号化コンテンツデータおよびローカルライセンスの複製および移動を禁止することを内容とするローカルライセンスを生成して、リッピングによって暗号化コンテンツデータおよびローカルライセンスを取得する。

【００４２】したがって、データ端末装置に入力されるコンテンツデータの種類に応じて暗号化コンテンツデータおよびローカルライセンスの複製内容を決定したローカルライセンスを生成できる。

【００４３】好ましくは、データ端末装置は、コンテン

ツデータを記録した記録媒体を駆動する媒体駆動手段をさらに備え、制御部は、媒体駆動手段が記録媒体から読出したコンテンツデータを暗号化コンテンツ生成手段へ与える。

【００４４】コンテンツデータが記録された記録媒体がデータ端末装置に装着されると、媒体駆動手段は、記録媒体からコンテンツデータを読出す。そして、制御部は、媒体駆動手段が読出したコンテンツデータを暗号化コンテンツ生成手段に与え、暗号化コンテンツ生成手段は、コンテンツデータに含まれる複製可否情報に応じてローカルライセンスを生成し、そのローカルライセンスに含まれるライセンス鍵によってコンテンツデータを暗号化して暗号化コンテンツデータを生成する。

【００４５】したがって、この発明によれば、媒体に記録されて頒布されたコンテンツデータから暗号化コンテンツデータおよびローカルライセンスを取得できる。

【００４６】好ましくは、データ端末装置の制御部は、インターネットによって受信したコンテンツデータを暗号化コンテンツ生成手段に与える。

【００４７】データ端末装置の制御部は、インターネットによって配信された平文のコンテンツデータを暗号化コンテンツ生成手段に与える。そして、暗号化コンテンツ生成手段は、コンテンツデータに含まれる複製可否情報に応じてローカルライセンスを生成し、そのローカルライセンスに含まれるライセンス鍵によってコンテンツデータを暗号化して暗号化コンテンツデータを生成する。なお、「インターネットによって受信したコンテンツデータ」とは、公開鍵等による暗号化を施して配信サーバとの間でデータのやり取り行なって受信したコンテンツデータを意味するものではなく、通常のインターネットによって配信されたコンテンツデータを意味する。

【００４８】したがって、この発明によれば、広く普及しているインターネットによって配信されるコンテンツデータから暗号化コンテンツデータおよびローカルライセンスを生成できる。

【００４９】好ましくは、データ端末装置の暗号化コンテンツ生成手段は、複製可否情報をコンテンツデータから検出する複製可否情報検出手段と、検出した複製可否情報を判定する複製可否情報判定手段と、複製可否情報判定手段の判定結果に基づいてローカルライセンスを生成するライセンス生成手段と、ライセンス鍵によってコンテンツデータを暗号化する暗号手段とを含む。

【００５０】データ端末装置に入力されたコンテンツデータは、暗号化コンテンツ生成手段に入力される。そして、暗号化コンテンツ生成手段においては、複製可否情報検出手段によってコンテンツデータから複製可否情報が検出され、複製可否情報判定手段によって複製可否情報の内容が判定される。そして、ライセンス生成手段は、複製可否情報判定手段による判定結果に応じてローカルライセンスを生成する。つまり、複製可否情報の内容がコンテンツデータの複製を許可するものであれば、ローカルライセンスの複製回数を設定したローカルライセンスを生成し、複製可否情報の内容がコンテンツデータの複製を禁止するものであるときは、ローカルライセンスを生成せず、複製可否情報が含まれていなければ、暗号化コンテンツデータおよびローカルライセンスの複製および移動を禁止したローカルライセンスを生成する。暗号手段は、生成されたローカルライセンスに含まれるライセンス鍵によってコンテンツデータを暗号化して暗号化コンテンツデータを生成する。

【００５１】したがって、この発明によれば、コンテンツデータに含まれる複製可否情報の内容に応じてローカルライセンスを生成し、暗号化コンテンツデータとローカルライセンスとをリッピングによって取得できる。

【００５２】好ましくは、データ端末装置の暗号化コンテンツ生成手段は、複製可否情報をコンテンツデータから検出する複製可否情報検出手段と、検出した複製可否情報を判定する複製可否情報判定手段と、複製可否情報判定手段の判定結果に基づいて複製条件を変更してコンテンツデータに書込む複製条件変更手段と、複製条件変更手段からのコンテンツデータを所定の方式に符号化する符号化手段と、複製可否情報判定手段の判定結果に基づいてローカルライセンスを生成するライセンス生成手段と、所定の方式に符号化されたコンテンツデータをライセンス鍵によって暗号化する暗号手段とを含む。

【００５３】データ端末装置に入力されたコンテンツデータは、暗号化コンテンツ生成手段に入力される。そして、暗号化コンテンツ生成手段においては、複製可否情報検出手段によってコンテンツデータから複製可否情報が検出され、複製可否情報判定手段によって複製可否情報の内容が判定される。そして、ライセンス生成手段は、複製可否情報判定手段による判定結果に応じてローカルライセンスを生成する。つまり、複製可否情報の内容がコンテンツデータの複製を許可するものであれば、ローカルライセンスの複製回数を設定したローカルライセンスを生成し、複製可否情報の内容がコンテンツデータの複製を禁止するものであるときは、ローカルライセンスを生成せず、複製可否情報が含まれていなければ、暗号化コンテンツデータおよびローカルライセンスの複製および移動を禁止したローカルライセンスを生成する。また、複製条件変更手段は、複製可否情報判定手段の判定結果に応じて複製条件を変更し、その変更した複製条件によってコンテンツデータに含まれる複製可否情報を書替える。そして、符号化手段は、複製可否情報が書替えられたコンテンツデータを所定の方式に符号化し、暗号手段は、生成されたローカルライセンスに含まれるライセンス鍵によってコンテンツデータを暗号化して暗号化コンテンツデータを生成する。

【００５４】したがって、この発明によれば、複製可否情報に中にコンテンツデータの利用規則を書込むことに

よって適法にコンテンツデータを複製することができる。

【００５５】好ましくは、データ端末装置のライセンス生成手段は、暗号化コンテンツデータを特定するコンテンツ識別子と、暗号化コンテンツデータおよびライセンスを他の装置へ貸出すときの通信を特定する通信識別子と、ライセンス鍵と、暗号化コンテンツデータおよびローカルライセンスを記録するデータ記録装置に対する記録装置アクセス条件と、ライセンスによって暗号化コンテンツデータを復号して再生するデータ再生装置に対する再生装置アクセス条件とから成るローカルライセンスを生成する。

【００５６】ライセンス生成手段は、ローカルライセンスを構成するコンテンツ識別子、通信識別子、ライセンス鍵、記録装置アクセス条件、および再生装置アクセス条件を生成する。

【００５７】したがって、この発明によれば、リッピングによって取得された暗号化コンテンツデータの他の装置への通信、および再生を保護するためのローカルライセンスを生成できる。

【００５８】好ましくは、コンテンツ識別子および通信識別子は、固定領域と、固定領域に続く管理領域とから成り、ライセンス生成手段は、コンテンツ識別子または通信識別子がデータ端末装置において生成されたことを示すローカル信号を固定領域に書込み、暗号化コンテンツデータに対応する識別番号を管理領域に書込んでコンテンツ識別子および通信識別子を生成する。

【００５９】ライセンス生成手段は、コンテンツ識別子および通信識別子の固定領域に、コンテンツ識別子および通信識別子がデータ端末装置において生成されたことを示すローカル信号を書込み、コンテンツ識別子および通信識別子の管理領域に、コンテンツやコンテンツデータの通信を特定するための個々の識別番号を書込む。

【００６０】したがって、この発明によれば、ローカルライセンスを構成するコンテンツ識別子および通信識別子の固定領域をみれば、そのライセンスがデータ端末装置で生成されたことが容易にわかる。

【００６１】好ましくは、データ端末装置のライセンス生成手段は、通信識別子とライセンス鍵とを乱数の発生によって生成する。

【００６２】ライセンス生成手段は、複製可否情報に基づいて乱数を発生させて通信識別しとライセンス鍵とを生成する。

【００６３】したがって、この発明によれば、外部から検出されにくい通信識別子およびライセンス鍵を生成できる。

【００６４】好ましくは、ローカルライセンスを構成する記録装置アクセス条件は、暗号化コンテンツデータの再生の可否および可能回数を表す再生可能回数と、暗号化コンテンツデータおよびローカルライセンスの移動および複製を制御する移動複製制御情報と、ローカルライセンスの保護レベルを表す保護レベル情報とから成る。

【００６５】暗号化コンテンツデータおよびローカルライセンスが記録されるデータ記録装置に対するアクセス条件として、暗号化コンテンツデータの再生可能回数、暗号化コンテンツデータおよびローカルライセンスの移動複製制御情報、およびローカルライセンスの保護レベルが生成される。

【００６６】したがって、この発明によれば、暗号化コンテンツデータの再生、移動および複製を再生可能回数や移動複製制御情報によって制御できる。また、保護レベルに応じてローカルライセンスを管理できる。

【００６７】好ましくは、記録装置アクセス条件を構成する再生可能回数は、暗号化コンテンツデータの再生不可を表す固定値から成る第１の再生可能回数と、暗号化コンテンツデータの再生を許諾する毎に単調減少する変動値から成る第２の再生可能回数と、暗号化コンテンツデータの再生を無制限に許諾する第３の再生可能回数とから成り、記録装置アクセス条件を構成する移動複製制御情報は、暗号化コンテンツデータおよびローカルライセンスの移動および複製を禁止する第１の制御情報と、暗号化コンテンツデータおよびローカルライセンスの移動を禁止し、暗号化コンテンツデータおよびローカルライセンスの複製を条件付きで許諾する第２の制御情報と、暗号化コンテンツデータおよびローカルライセンスの移動および複製を条件付きで許諾する第３の制御情報と、暗号化コンテンツデータおよびローカルライセンスの移動を許可し、暗号化コンテンツデータおよびローカルライセンスの複製を禁止する第４の制御情報と、暗号化コンテンツデータおよびローカルライセンスの移動および複製を無制限に許諾する第５の制御情報とから成る。

【００６８】したがって、この発明によれば、暗号化コンテンツデータの再生と、暗号化コンテンツデータおよびローカルライセンスの移動および複製とを詳細に制御できる。

【００６９】好ましくは、移動複製制御情報の第２の制御情報は、暗号化コンテンツデータおよびローカルライセンスの複製毎に単調減少し、かつ、複製可能回数を表す変動値を含み、移動複製制御情報の第３の制御情報は、暗号化コンテンツデータおよびローカルライセンスの移動および複製毎に単調増加する変動値を含む。

【００７０】したがって、この発明によれば、暗号化コンテンツデータおよびライセンスの移動および複製の各内容に応じた方法によって暗号化コンテンツデータおよびライセンスの移動および複製を制御できる。

【００７１】好ましくは、再生装置アクセス条件は、暗号化コンテンツデータの再生速度の変換可否を示す第１の信号と、暗号化コンテンツデータの編集の可否を示す第２の信号と、再生可能な暗号化コンテンツデータのサ

イズを示す第３の信号と、暗号化コンテンツデータの利用最終日時を示す第４の信号と、暗号化コンテンツデータの利用開始日時を示す第５の信号と、地域コードとから成る。

【００７２】したがって、この発明によれば、暗号化コンテンツデータの再生を詳細に制御できる。

【００７３】好ましくは、貸出情報は、暗号化コンテンツデータおよびローカルライセンスの貸出しを禁止する禁止情報と、暗号化コンテンツデータおよびローカルライセンスの貸出し毎に単調減少し、暗号化コンテンツデータおよびローカルライセンスの返却毎に単調増加する貸出許可情報とから成る。

【００７４】したがって、この発明によれば、リッピングによって取得した暗号化コンテンツデータおよびローカルライセンスの他の装置への貸出しを正確に制御できる。

【００７５】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００７６】図１は、本発明によるデータ端末装置（パーソナルコンピュータ）が暗号化コンテンツデータを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００７７】なお、以下では携帯電話網を介してデジタル音楽データをユーザの携帯電話に装着されたメモリカード１１０に、またはインターネットを介してデジタル音楽データを各パーソナルコンピュータに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【００７８】図１を参照して、配信キャリア２０は、自己の携帯電話網を通じて得た、ユーザからの配信要求（配信リクエスト）を配信サーバ１０に中継する。著作権の存在する音楽データを管理する配信サーバ１０は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機１００に装着されたメモリカード１１０が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報として暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスを与える。

【００７９】配信キャリア２０は、自己の携帯電話網を通じて配信要求を送信した携帯電話機１００に装着されたメモリカード１１０に対して、携帯電話網および携帯電話機１００を介して暗号化コンテンツデータとライセンスとを配信する。

【００８０】図１においては、たとえば携帯電話ユーザの携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機１００中の音楽再生部（図示せず）に与える。

【００８１】さらに、たとえば携帯電話ユーザは、携帯電話機１００に接続したヘッドホーン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【００８２】このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ１０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００８３】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００８４】また、図１においては、配信サーバ１０は、モデム４０およびインターネット網３０を通じて得た、パーソナルコンピュータのユーザからの配信要求を受信する。そうすると、配信サーバ１０は、データ配信を求めてアクセスして来たパーソナルコンピュータ５０が正当な認証データを持つライセンス管理モジュールを備えたソフトウェアを利用してアクセスしているか否か、すなわち、正規のライセンス管理モジュールであるか否かの認証処理を行ない、正当なライセンス管理モジュールを備えたパーソナルコンピュータに対して所定の暗号方式により音楽データを暗号化した上で、このような暗号化コンテンツデータおよびライセンスをインターネット網３０およびモデム４０を介して送信する。パーソナルコンピュータ５０のライセンス管理モジュールは受信した暗号化コンテンツデータをハードディスク（ＨＤＤ）等にそのまま記録し、受信したライセンスは、暗号化して保護した上で、ＨＤＤに記録する。

【００８５】パーソナルコンピュータ５０は、メモリカード１１０のライセンス管理モジュールのライセンス管理に関わる機能と同一機能を備えたライセンス管理デバイス（ハードウェア）を備えることで、ＨＤＤに記録したセキュリティレベルより高いセキュリティレベルで、すなわち、携帯電話機１００およびメモリカード１１０を用いて受信したのと同じセキュリティレベルの配信を受けることができる。モデム４０およびインターネット

網３０を介して、配信サーバ１０から、暗号化コンテンツデータとライセンスとを配信サーバ１０から受信する。このとき、ライセンスは、配信サーバ１０とライセンス管理モジュールとの間で所定の手順に従った暗号通信路を用いて、直接、ライセンス管理デバイスにおいて受信され、記録される。暗号化コンテンツデータはそのままＨＤＤに記録される。このライセンス管理デバイスは、メモリカード１１０と同じようにライセンスの送受信や管理の機密性をハード的に保持するものであり、機密性をソフトウェアで保持するライセンス管理モジュールに比べてセキュリティレベルが高いものである。セキュリティレベルおよびライセンスを区別するためにメモリカード１１０あるいはライセンス管理デバイスなどのハードウェアによって機密性を保つセキュリティレベルをレベル２と呼び、レベル２のセキュリティを要求して配信されたライセンスをレベル２ライセンスと呼ぶこととする。同様に、ライセンス管理モジュールのようなソフトウェアによって機密性を保つセキュリティレベルをレベル１と呼び、レベル１のセキュリティレベルを要求して配信されたライセンスをレベル１ライセンスと呼ぶこととする。ライセンス管理デバイスおよびライセンス管理モジュールについては、後に詳細に説明する。

【００８６】さらに、図１においては、パーソナルコンピュータ５０は、ライセンス管理モジュールを使って音楽データを記録した音楽ＣＤ（Ｃｏｍｐａｃｔ　Ｄｉｓｋ）６０から取得した音楽データからローカル使用に限定された暗号化コンテンツデータと、暗号化コンテンツデータを再生するためのライセンスとを生成する。この処理をリッピングと呼び、音楽ＣＤから暗号化コンテンツデータとライセンスとを取得する行為に相当する。リッピングによるローカル使用のライセンスは、その性格上、セキュリティレベルは決して高くないので、リッピングが如何なる手段でなされようともレベル１ライセンスとして扱われるものとする。リッピングの詳細については後述する。

【００８７】またさらに、パーソナルコンピュータ５０は、ＵＳＢ（ＵｎｉｖｅｒｓａｌＳｅｒｉａｌ　Ｂｕｓ）ケーブル７０によって携帯電話機１００と接続し、暗号化コンテンツデータおよびライセンスを携帯電話機１００に装着されたメモリカード１１０と送受信することが可能である。しかしながら、ライセンスのセキュリティレベルによってその扱いは異なる。詳細については後述する。

【００８８】更に、図１においては、パーソナルコンピュータ５０は、ライセンス管理モジュールを使って、ライセンス管理モジュールが直接管理するレベル１ライセンスを持つ暗号化コンテンツデータに限り、再生する機能を備えることができる。レベル２ライセンスを持つ暗号化コンテンツデータの再生は、ハードウェアによって機密性を持つコンテンツ再生回路をパーソナルコンピュータに備えれば可能となる。パーソナルコンピュータにおける再生についての詳細な説明は、本出願における説明を簡略化するために省略する。

【００８９】したがって、図１に示すデータ配信システムにおいては、パーソナルコンピュータ５０は、モデム４０およびインターネット網３０を介して配信サーバ１０から暗号化コンテンツデータとライセンスとを受信するとともに、音楽ＣＤから暗号化コンテンツデータとライセンスとを取得する。また、携帯電話機１００に装着されたメモリカード１１０は、携帯電話網を介して配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信するとともに、パーソナルコンピュータ５０が配信サーバ１０または音楽ＣＤ６０から取得した暗号化コンテンツデータおよびライセンスを受信する。携帯電話機１００のユーザは、パーソナルコンピュータ５０を介することによって音楽ＣＤから暗号化コンテンツデータおよびライセンスを取得することが可能となる。

【００９０】さらに、携帯電話機１００に装着されたメモリカード１１０は、携帯電話網を介して配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ５０に待避することが可能となる。

【００９１】図２は、携帯電話網を介して配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信する機能を有しない再生端末１０２を用いた場合のデータ配信システムを示したものである。図２に示すデータ配信システムにおいては、再生端末１０２に装着されたメモリカード１１０は、パーソナルコンピュータ５０が配信サーバ１０または音楽ＣＤ６０から取得した暗号化コンテンツデータおよびライセンスを受信する。このように、パーソナルコンピュータ５０が暗号化コンテンツデータおよびライセンスを取得することによって通信機能のない再生端末１０２のユーザも暗号化コンテンツデータを受信することができるようになる。

【００９２】図１および図２に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話またはパーソナルコンピュータのユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、さらに第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【００９３】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機またはパーソナルコンピュータとも言う。以下同じ）に対するコンテンツデータ

の出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００９４】なお、以下の説明においては、配信サーバ１０から、各携帯電話機、各パーソナルコンピュータ等にコンテンツデータを伝送する処理を「配信」と称することとする。

【００９５】図３は、図１および図２に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００９６】まず、配信サーバ１０より配信されるデータについて説明する。Ｄｃは、音楽データ等のコンテンツデータである。コンテンツデータＤｃは、ライセンス鍵Ｋｃで復号可能な暗号化が施される。ライセンス鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃがこの形式で配信サーバ１０より携帯電話またはパーソナルコンピュータのユーザに配布される。

【００９７】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００９８】さらに、配信サーバ１０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄｃ－ｉｎｆが配布される。また、ライセンスとして、ライセンス鍵Ｋｃ、配信サーバ１０からのライセンス鍵等の配信を特定するための管理コードであるトランザクションＩＤが配信サーバ１０と携帯電話機１００との間、または配信サーバ１０とパーソナルコンピュータ５０との間でやり取りされる。また、配信によらないライセンス、すなわち、ローカルでの使用を目的とするライセンスを特定するためにもトランザクションＩＤは使用される。配信によるものと、ローカル使用のものとを区別するために、トランザクションＩＤの先頭は“０”で始まるものがローカル使用のトランザクションＩＤであり、“０”以外から始まるのものを配信によるトランザクションＩＤであるとする。さらに、ライセンスとしては、コンテンツデータＤｃを識別するためのコードであるコンテンツＩＤや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、記録装置（メモリカード、またはライセンス管理デバイス）におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報ＡＣｍおよびデータ再生端末における再生に関する制御情報である再生制御情報ＡＣｐ等が存在する。具体的には、アクセス制御情報ＡＣｍはメモリカード、ライセンス管理モジュールおよびライセンス管理デバイスからのライセンスまたはライセンス鍵を外部に出力するに当っての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報およびライセンスのセキュリティレベルなどがある。再生制御情報ＡＣｐは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【００９９】以後、トランザクションＩＤとコンテンツＩＤとを併せてライセンスＩＤと総称し、ライセンス鍵Ｋｃとライセンスｉｄとアクセス制御情報ＡＣｍと再生制御情報ＡＣｐとを併せて、ライセンスと総称することとする。

【０１００】また、以降では、簡単化のためアクセス制御情報ＡＣｍは再生回数の制限を行なう制御情報である再生回数（０：再生不可、１～２５４：再生可能回数、２５５：制限無し）、ライセンスの移動および複製を制限する移動・複製フラグ（０：移動複製禁止、１：移動のみ可、２：移動複製可）の２項目とし、再生制御情報ＡＣｐは再生可能な期限を規定する制御情報である再生期限（ＵＴＣｔｉｍｅコード）のみを制限するものとする。

【０１０１】本発明の実施の形態においては、記録装置（メモリカード、またはライセンス管理デバイス）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストＣＲＬ（Ｃｌａｓｓ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）の運用を行なう。以下では、必要に応じて記号ＣＲＬによって禁止クラスリスト内のデータを表わすこともある。

【０１０２】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止される携帯電話機、メモリカード、パーソナルコンピュータ上のライセンス管理モジュール、およびライセンス管理デバイスのクラスをリストアップした禁止クラスリストデータＣＲＬが含まれる。コンテンツデータ保護にかかわるライセンスの管理・蓄積および再生を行なう全ての機器およびプログラムがリストアップの対象となる。

【０１０３】禁止クラスリストデータＣＲＬは、配信サーバ１０内で管理されるとともに、メモリカードまたはライセンス管理デバイス内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび／またはライセンス鍵等のライセンスを配信する際に、携帯電話機またはパーソナルコンピュータ（ライセンス管理デバイスまたはライセンス管理モジュール）から受取った禁止クラスリストの更新日時を判断し、所有する禁止クラスリストＣＲＬの更新日時と比較して更新されていないと判断されたとき、更新された禁止クラスリストを携帯電話機またはパーソナルコンピュータに配信する。また、禁止クラスリストの変更については、変更点のみを反映した差分データである差分ＣＲＬを配信サーバ１０

側より発生して、これに応じてメモリカードまたはライセンス管理デバイス内の禁止クラスリストＣＲＬに追加する構成とすることも可能である。また、メモカードまたはライセンス管理デバイス内で管理される禁止クラスリストＣＲＬには更新日時ＣＲＬｄａｔｅも更新時に記録されているものとする。

【０１０４】このように、禁止クラスリストＣＲＬを、配信サーバのみならずライセンスを記録して管理するライセンス管理装置（メモリカードまたはライセンス管理デバイス）またはライセンス管理モジュールにおいても保持運用することによって、再生やライセンスの移動・複製・チェックアウトなどに際して、クラス固有すなわち、コンテンツ再生回路（携帯電話機および再生端末）、ライセンス管理装置またはライセンス管理モジュールの種類に固有の復号鍵が破られた、コンテンツ再生回路（携帯電話機および再生端末）、ライセンス管理装置またはパーソナルコンピュータ上で動作しているライセンス管理モジュールへのライセンス鍵あるいはライセンスの供給を禁止する。このため、携帯電話機またはパーソナルコンピュータではコンテンツデータの再生が、メモリカードまたはパーソナルコンピュータではライセンス管理デバイスに対して、あるいはライセンス管理モジュールを介してライセンスの取得が行なえなくなり、新たなコンテンツデータを受信することができなくなる。

【０１０５】このように、メモリカードまたはライセンス管理デバイス内の、あるいはライセンス管理モジュールが管理する禁止クラスリストＣＲＬは配信時に逐次データを更新する構成とする。また、メモリカードまたはライセンス管理デバイス内における禁止クラスリストＣＲＬの管理は、上位レベルとは独立にメモリカードまたはライセンス管理デバイス内では、ハード的に機密性を保証する高いレベルの耐タンパモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｔ　Ｍｏｄｕｌｅ）に記録する。ライセンス管理モジュールにおける禁止クラスリストＣＲＬの管理は、暗号処理によって少なくとも改ざん防止処置が行われてパーソナルコンピュータのＨＤＤ等に記録される。言いかえれば、ソフトウェアによってその機密性が保証された低いレベルの耐タンパモジュールによって記録される。したがって、ファイルシステムやアプリケーションプログラム等の上位レベルから禁止クラスリストデータＣＲＬを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【０１０６】図４は、図１および図２に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【０１０７】コンテンツ再生回路、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールには固有の公開暗号鍵ＫＰｐｙおよびＫＰｍｗがそれぞれ設けられ、公開暗号鍵ＫＰｐｙおよびＫＰｍｗはコンテンツ再生回路に固有の秘密復号鍵Ｋｐｙおよびメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールに固有の秘密復号鍵Ｋｍｗによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、コンテンツ再生デバイス、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【０１０８】また、コンテンツ再生回路（携帯電話機、再生端末）のクラス証明書としてＣｐｙが設けられ、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書としてＣｍｗが設けられる。これらのクラス証明書は、コンテンツ再生回路、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラスごとに異なる情報を有する。耐タンパモジュールが破られたり、クラス鍵による暗号が破られた、すなわち、秘密復号鍵が漏洩したクラスに対しては、禁止クラスリストにリストアップされてライセンス取得の禁止対象となる。

【０１０９】これらのコンテンツ再生回路のクラス公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｐｙ／／Ｃｐｙ｝ＫＰａの形式で、メモリカード、およびライセンス管理デバイスのクラス公開暗号鍵およびクラス証明書は認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａの形式で、ライセンス管理モジュールのクラス公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰｂの形式で、出荷時にデータ再生回路、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールにそれぞれ記録される。後ほど詳細に説明するが、ＫＰａ、ＫＰｂは配信システム全体で共通の公開認証鍵であり、ＫＰａはセキュリティレベルがレベル２である場合に、ＫＰｂはセキュリティレベルがレベル１である場合に用いられる。

【０１１０】また、メモリカード１１０、ライセンス管理デバイス、およびライセンス管理モジュール内のデータ処理を管理するための鍵として、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールという媒体または管理ソフトウェアごとに設定される公開暗号鍵ＫＰｍｃｘと、公開暗号鍵ＫＰｍｃｘで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Ｋｍｃｘが存在する。このメモリカードごとに個別な公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵ＫＰｍｃｘを個別公開暗号鍵、秘密復号鍵Ｋｍｃｘを個別秘密復号鍵と称する。

【０１１１】メモリカード外とメモリカード間でのデー

タ授受、またはライセンス管理デバイス外とライセンス管理デバイス間でのデータ授受、またはライセンス管理モジュール外とライセンス管理モジュール間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ１０、携帯電話機１００、メモリカード１１０、ライセンス管理デバイス、ライセンス管理モジュールにおいて生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【０１１２】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、コンテンツ再生回路もしくはメモリカードもしくはライセンス管理デバイスもしくはライセンス管理モジュール間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【０１１３】これらのセッションキーＫｓ１～Ｋｓ３は、各セッションごとに固有の値を有することにより、配信サーバ、コンテンツ再生回路、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカード、ライセンス管理デバイス、ライセンス管理モジュールによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、コンテンツ再生回路において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【０１１４】図５は、図１および図２に示した配信サーバ１０の構成を示す概略ブロック図である。

【０１１５】配信サーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツＩＤ等の配信情報を保持するための情報データベース３０４と、携帯電話やパーソナルコンピュータの各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、禁止クラスリストＣＲＬを管理するＣＲＬデータベース３０６と、情報データベース３０４に保持されたコンテンツデータのメニューを保持するメニューデータベース３０７と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクションＩＤ等の配信に関するログを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、ＣＲＬデータベース３０６、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【０１１６】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ｛ＫＰmw／／Ｃmw｝ＫＰａまたは｛ＫＰmw／／Ｃmw｝ＫＰｂを復号するための２種類の公開認証鍵ＫＰａとＫＰｂを保持する認証鍵保持部３１３と、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ｛ＫＰmw／／Ｃmw｝ＫＰａまたは｛ＫＰmw／／Ｃmw｝ＫＰｂを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰａまたはＫＰｂによって復号処理を行なう復号処理部３１２と、配信セッションごとに、セッション鍵Ｋｓ１を発生するセッションキー発生部３１６、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られたクラス公開暗号鍵ＫＰmwを用いて暗号化して、バスＢＳ１に出力するための暗号化処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【０１１７】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよびアクセス制御情報ＡＣｍを、復号処理部３２０によって得られたメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールごとに個別公開暗号鍵ＫＰｍｃｘによって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号化処理部３２８とを含む。

【０１１８】配信サーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１１９】図６は、図１および図２に示したパーソナルコンピュータ５０の構成を説明するための概略ブロック図である。パーソナルコンピュータ５０は、パーソナルコンピュータ５０の各部のデータ授受を行なうためのバスＢＳ２と、パーソナルコンピュータ内を制御すると共に、各種のプログラムを実行するためのコントローラ（ＣＰＵ）５１０と、データバスＢＳ２と、データバスＢＳ２に接続され、プログラムやデータを記録し、蓄積しておくための大容量記録装置であるハードディスク（ＨＤＤ）５３０およびＣＤ－ＲＯＭドライブ５４０と、ユーザからの指示を入力するためのキーボード５６

０と、各種の情報を視覚的にユーザに与えるためのディスプレイ５７０とを含む。

【０１２０】パーソナルコンピュータ５０は、さらに、暗号化コンテンツデータおよびライセンスを携帯電話機１００等へ通信する際にコントローラ５１０と端子５８０との間でデータの授受を制御するためのＵＳＢインタフェース５５０と、ＵＳＢケーブル７０を接続するための端子５８０と、配信サーバ１０とインターネット網３０およびモデム４０を介して通信する際にコントローラ５１０と端子５８５との間でデータの授受を制御するためのシリアルインタフェース５５５と、モデム４０とケーブルで接続するための端子５８５とを含む。

【０１２１】コントローラ５１０は、インターネット網４０を介してライセンス管理デバイス５２０またはライセンス管理モジュール５１１に暗号化コンテンツデータ等を配信サーバ１０から受信するために、配信サーバ１０との間でデータの授受を制御するとともに、ＣＤ－ＲＯＭドライブ５４０を介して音楽ＣＤからリッピングによって暗号化コンテンツデータおよびライセンスを取得する際の制御を行なう。さらに、パーソナルコンピュータ５０は、配信サーバ１０からの暗号化コンテンツデータおよびライセンスの受信を行なう際に配信サーバ１０との間で各種の鍵のやり取りを行ない、配信された暗号化コンテンツデータを再生するためのライセンスをハード的に管理するライセンス管理デバイス５２０と、コントローラ５１０にて実行されるプログラムであって、配信サーバ１０からの暗号化コンテンツデータおよびレベル１ライセンスの配信を受信し、その受信したライセンスに独自の暗号化を施した専用ライセンスを生成するコンテンツ管理モジュール５１１とを含む。

【０１２２】ライセンス管理デバイス５２０は、暗号化コンテンツデータおよびライセンスを配信サーバ１０から受信する際のデータの授受をハード的に行ない、受信したライセンスをハード的に管理するものであるため、高いセキュリティレベルを要求するレベル２のライセンスを扱うことができる。一方、ライセンス管理モジュール５１１は、暗号化コンテンツデータおよびライセンスを配信サーバ１０から受信する際のデータの授受をコントローラ５１０にて実行されるプログラムを用いてソフト的に行ない、また、音楽ＣＤからリッピングによってローカル使用の暗号化コンテンツデータおよびライセンスの生成を行い、取得したライセンスに対して暗号処理などを施して保護し、ＨＤＤ５３０に蓄積して管理するものであり、ライセンス管理デバイス５２０よりもセキュリティレベルが低い、レベル１ライセンスのみを扱う。なお、高いセキュリティレベルがレベル２である場合にはレベル１ライセンスも扱えることは言うまでもない。

【０１２３】このように、パーソナルコンピュータ５０は、配信サーバ１０からインターネット網３０を介して暗号化コンテンツデータおよびライセンスを受信するためのライセンス管理モジュール５１１およびライセンス管理デバイス５２０と、音楽ＣＤからリッピングによって暗号化コンテンツデータおよびライセンスを取得するためのＣＤ－ＲＯＭドライブ５４０とを内蔵するものである。

【０１２４】図７は、図２に示した再生端末１０２の構成を説明するための概略ブロック図である。

【０１２５】再生端末１０２は、再生端末１０２の各部のデータ授受を行なうためのバスＢＳ３と、バスＢＳ３を介して再生端末１０２の動作を制御するためのコントローラ１１０６と、外部からの指示を再生端末１０２に与えるための操作パネル１１０８と、コントローラ１１０６等から出力される情報をユーザに視覚情報として与えるための表示パネル１１１０とを含む。

【０１２６】再生端末１０２は、さらに、配信サーバ１０からのコンテンツデータ（音楽データ）を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード１１０と、メモリカード１１０とバスＢＳ３との間のデータの授受を制御するためのメモリインタフェース１２００と、パーソナルコンピュータ５０から暗号化コンテンツデータおよびライセンスを受信する際にバスＢＳ３と端子１１１４との間のデータ授受を制御するためのＵＳＢインタフェース１１１２と、ＵＳＢケーブル７０を接続するための端子１１１４とを含む。

【０１２７】再生端末１０２は、さらに、クラス公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｐ１を公開認証鍵ＫＰａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを保持する認証データ保持部１５００を含む。ここで、再生端末１０２のクラスｙは、ｙ＝１であるとする。

【０１２８】再生端末１０２は、さらに、クラス固有の復号鍵であるＫｐ１を保持するＫｐ１保持部１５０２と、バスＢＳ３から受けたデータをＫｐ１によって復号し、メモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１５０４とを含む。

【０１２９】再生端末１０２は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でバスＢＳ３上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１５０８と、暗号化コンテンツデータの再生セッションにおいてメモリカード１１０からライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを受取る際に、セッションキー発生部１５０８により発生されたセッションキーＫｓ３を復号処理部１５０４によって得られたセッションキーＫｓ２によって暗号化し、バスＢＳ３に出力する暗号化処理部１５０６とを含む。

【０１３０】再生端末１０２は、さらに、バスＢＳ３上のデータをセッションキーＫｓ３によって復号して、ラ

イセンス鍵Ｋｃおよび再生制御情報ＡＣｐを出力する復号処理部１５１０と、バスＢＳ３より暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受けて、復号処理部１５１０より取得したライセンス鍵Ｋｃによって復号し、コンテンツデータを出力する復号処理部１５１６と、復号処理部１５１６の出力を受けてコンテンツデータを再生するための音楽再生部１５１８と、音楽再生部１５１８の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１５１９と、ＤＡ変換器１５１９の出力をヘッドホーンなどの外部出力装置（図示省略）へ出力するための端子１５３０とを含む。

【０１３１】なお、図７においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス１５５０を構成する。

【０１３２】一方、図１に示す携帯電話機１００は、携帯電話網を介して配信サーバ１０から暗号化コンテンツデータあるいはライセンスの配信を受信する機能を有するものである。したがって、図１に示す携帯電話機１００の構成は、図７に示す構成において、携帯電話網により無線伝送される信号を受信するためのアンテナと、アンテナからの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナに与えるための送受信部とマイクとスピーカと音声コーデック等の携帯電話機が本来備える機能を設けたものである。

【０１３３】携帯電話機１００、再生端末１０２の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１３４】図８は、図１および図２に示すメモリカード１１０の構成を説明するための概略ブロック図である。

【０１３５】既に説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、ＫＰmwおよびＫmwが設けられ、メモリカードのクラス証明書Ｃmwが設けられるが、メモリカード１１０においては、自然数ｗ＝３で表わされるものとする。また、メモリカードを識別する自然数ｘはｘ＝４で表されるものとする。

【０１３６】したがって、メモリカード１１０は、認証データ｛ＫＰm３／／Ｃm３｝ＫＰａを保持する認証データ保持部１４００と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Ｋmｃ４を保持するＫmｃ保持部１４０２と、クラス秘密復号鍵Ｋm３を保持するＫm保持部１４２１と、個別秘密復号鍵Ｋmｃ４によって復号可能な公開暗号鍵ＫＰmｃ４を保持するＫＰmｃ保持部１４１６とを含む。

【０１３７】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【０１３８】メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１４２６を介して授受するインタフェース１４２４と、インタフェース１４２４との間で信号をやり取りするバスＢＳ４と、バスＢＳ４にインタフェース１４２４から与えられるデータから、クラス秘密復号鍵Ｋm３をＫm保持部１４２１から受けて、配信サーバ１０が配信セッションにおいて生成したセッションキーＫｓ1を接点Ｐａに出力する復号処理部１４２２と、ＫＰａ保持部１４１４から公開認証鍵ＫＰａを受けて、バスＢＳ４に与えられるデータから公開認証鍵ＫＰａによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ１４２０に、得られたクラス公開鍵を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４６によって選択的に与えられるデータを暗号化してバスＢＳ４に出力する暗号化処理部１４０６とを含む。

【０１３９】メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られるクラス公開暗号鍵ＫＰｐｙもしくはＫＰmwによって暗号化してバスＢＳ４に送出する暗号化処理部１４１０と、バスＢＳ４よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号する復号処理部１４１２と、暗号化コンテンツデータの再生セッションにおいてメモリ１４１５から読出されたライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを、復号処理部１４１２で復号された他のメモリカード１１０の個別公開暗号鍵ＫＰmｃｘ（≠４）で暗号化する暗号処理部１４１７とを含む。

【０１４０】メモリカード１１０は、さらに、バスＢＳ４上のデータを個別公開暗号鍵ＫＰmｃ４と対をなすメモリカード１１０の個別秘密復号鍵Ｋmｃ４によって復号するための復号処理部１４０４と、禁止クラスリストのバージョン更新のためのデータＣＲＬ＿ｄａｔによって逐次更新される禁止クラスリストデータＣＲＬと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生するためのライセンス（Ｋｃ，ＡＣｐ，ＡＣm，ライセンスＩＤ）と、付加情報Ｄａｔａ－ｉｎｆと、暗号化コンテンツデータの再生リストと、ライセンスを管理するためのライセンス管理ファイルとをバスＢＳ４より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。また、メモリ１５１５は、ＣＲＬ領域１４１５Ａと、ライセンス領域１４１５Ｂと、データ領域１４１５Ｃとから成る。ＣＲＬ領域１４１５Ａは、禁止クラスリストＣＲＬを記録するための領域であ

る。ライセンス領域１４１５Ｂは、ライセンスを記録するための領域である。データ領域１４１５Ｃは、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、暗号化コンテンツデータの関連情報Ｄｃ－ｉｎｆ、ライセンスを管理するために必要な情報を暗号化コンテンツごとに記録するライセンス管理ファイル、およびメモリカードに記録された暗号化コンテンツデータやライセンスにアクセスするための基本的な情報を記録する再生リストファイルを記録するための領域である。そして、データ領域１４１５Ｃは、外部から直接アクセスが可能である。ライセンス管理ファイルおよび再生リストファイルの詳細については後述する。

【０１４１】ライセンス領域１４１５Ｂは、ライセンス（ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、アクセス制限情報ＡＣｍ、ライセンスＩＤ）を記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスを格納する。ライセンスに対してアクセスする場合には、ライセンスか格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

【０１４２】メモリカード１１０は、さらに、バスＢＳ４を介して外部との間でデータ授受を行ない、バスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０を含む。

【０１４３】なお、データ領域１４１５Ｃを除く全ての構成は、耐タンパモジュール領域に構成される。

【０１４４】図９は、パーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５２０の構成を示す概略ブロック図である。ライセンス管理デバイス５２０は、メモカード１１０におけるデータ領域１４１５Ｃに相当する領域を必要としない点、インタフェース１４２４の機能および端子１４２６の形状が異なるインタフェース５２２４と端子５２２６とを備える点が異なるのみで、基本的にメモリカード１１０と同じ構成から成る。ライセンス管理デバイス５２０の認証データ保持部５２００、Ｋｍｃ保持部５２０２、復号処理部５２０４、暗号処理部５２０６、復号処理部５２０８、暗号処理部５２１０、復号処理部５２１２、ＫＰａ保持部５２１４、ＫＰｍｃ保持部５２１６、暗号処理部５２１７、セッションキー発生部５２１８、コントローラ５２２０、Ｋｍ保持部５２２１、復号処理部５２２２、インタフェース５２２４、端子５２２６、切換スイッチ５２４２，５２４６は、それぞれ、メモリカード１１０の認証データ保持部１４００、Ｋｍｃ保持部１４０２、復号処理部１４０４、暗号処理部１４０６、復号処理部１４０８、暗号処理部１４１０、復号処理部１４１２、ＫＰａ保持部１４１４、ＫＰｍｃ保持部１４１６、暗号処理部１４１７、セッションキー発生部１４１８、コントローラ１４２０、Ｋｍ保持部１４２１、復号処理部１４２２、切換スイッチ１４４２，１４４６と同じである。ただし、認証データ保持部５２００は、認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａを保持し、ＫＰｍｃ保持部５２１６は、個別公開暗号鍵ＫＰｍ８を保持し、Ｋｍ保持部５２０２は、クラス秘密復号鍵Ｋｍ７を保持し、Ｋｍｃ保持部５２２１は、個別秘密復号鍵Ｋｍｃ８を保持する。ライセンス管理デバイス５２０のクラスを表す自然数ｗはｗ＝７であり、ライセンス管理デバイス５２０を識別するための自然数ｘはｘ＝８であるとする。

【０１４５】ライセンス管理デバイス５２０は、禁止クラスリストＣＲＬとライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ）とを記録するメモリ５２１５を、メモリカード１１０のメモリ１４１５に代えて含む。メモリ５２１５は、禁止クラスリストＣＲＬを記録したＣＲＬ領域５２１５Ａと、ライセンスを記録したライセンス領域５２１５Ｂとから成る。

【０１４６】以下、図１および図２に示すデータ配信システムにおける各セッションの動作について説明する。

【０１４７】［配信１］まず、図１および図２に示すデータ配信システムにおいて、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理デバイス５２０へ暗号化コンテンツデータおよびライセンスを配信する動作について説明する。なお、この動作を「配信１」という。

【０１４８】図１０～図１３は、図１および図２に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生するパーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５２０への配信動作（以下、配信セッションともいう）を説明するための第１～第４のフローチャートである。

【０１４９】図１０における処理以前に、パーソナルコンピュータ５０のユーザは、配信サーバ１０に対してモデム４０を介して接続し、購入を希望するコンテンツに対するコンテンツＩＤを取得していることを前提としている。

【０１５０】図１０を参照して、パーソナルコンピュータ５０のユーザからキーボード５６０を介してコンテンツＩＤの指定による配信リクエストがなされる（ステップＳ１００）。そして、キーボード５６０を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣが入力される（ステップＳ１０２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータのアクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐを設定して購入条件ＡＣが入力される。

【０１５１】暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ５１０は、バスＢＳ２を介してライセンス管理デバイス５２０へ認証データの出力指示を与える（ステップＳ１０４）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４およびバスＢＳ５を介して

認証データの出力指示を受取る。そして、コントローラ５２２０は、バスＢＳ５を介して認証データ保持部５２００から認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａを読出し、｛ＫＰｍ７／／Ｃｍ７｝ＫＰａをバスＢＳ５、インタフェース５２２４および端子５２２６を介して出力する（ステップＳ１０６）。

【０１５２】パーソナルコンピュータ５０のコントローラ５１０は、ライセンス管理デバイス５２０からの認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣ、および配信リクエストを配信サーバ１０に対して送信する（ステップＳ１０８）。

【０１５３】配信サーバ１０では、パーソナルコンピュータ５０から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ、およびライセンス購入条件のデータＡＣを受信し（ステップＳ１１０）、復号処理部３１２においてライセンス管理デバイス５２０から出力された認証データを公開認証鍵ＫＰａで復号処理を実行する（ステップＳ１１２）。

【０１５４】配信制御部３１５は、復号処理部３１２における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１４）。正当な認証データであると判断された場合、配信制御部３１５は、クラス公開暗号鍵ＫＰｍ７およびクラス証明書Ｃｍ７を承認し、受理する。そして、次の処理（ステップＳ１１６）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ７およびクラス証明書Ｃｍ７を受理しないで配信セッションを終了する（ステップＳ１９８）。

【０１５５】認証の結果、クラス公開暗号鍵ＫＰｍ７およびクラス証明書Ｃｍ７を受理すると、配信制御部３１５は、次に、ライセンス管理デバイスのクラス証明書Ｃｍ７が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１９８）。

【０１５６】一方、ライセンス管理デバイス５２０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ１１６）。

【０１５７】認証の結果、正当な認証データを持つライセンス管理デバイスを備えるパーソナルコンピュータからのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ１０において、配信制御部３１５は、配信を特定するための管理コードであるトランザクションＩＤを生成する（ステップＳ１１８）。また、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ１２０）。セッションキーＫｓ１は、復号処理部３１２によって得られたライセンス管理デバイス５２０に対応するクラス公開暗号鍵ＫＰｍ７によって、暗号化処理部３１８によって暗号化される（ステップＳ１２２）。

【０１５８】トランザクションＩＤおよび暗号化されたセッションキーＫｓ１は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ７として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１２４）。

【０１５９】図１１を参照して、パーソナルコンピュータ５０が、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ７を受信すると（ステップＳ１２６）、コントローラ５１０は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ７をライセンス管理デバイス５２０に入力する（ステップＳ１２８）。そうすると、ライセンス管理デバイス５２０においては、端子５２２６およびインタフェース５２２４を介して、バスＢＳ５に与えられた受信データを、復号処理部５２２２が、保持部５２２１に保持されるライセンス管理デバイス５２０に固有なクラス秘密復号鍵Ｋｍ７によって復号処理することにより、セッションキーＫｓ１を復号し、セッションキーＫｓ１を受理する（ステップＳ１３０）。

【０１６０】コントローラ５２２０は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部５２１８に対してライセンス管理デバイス５２０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。そして、セッションキー発生部５２１８は、セッションキーＫｓ２を生成する（ステップＳ１３２）。

【０１６１】また、配信セッションにおいては、コントローラ５２２０は、ライセンス管理デバイス５２０内のメモリ５２１５に記録されている禁止クラスリストＣＲＬから更新日時ＣＲＬｄａｔｅを抽出して切換スイッチ５２４６に出力する（ステップＳ１３４）。

【０１６２】暗号化処理部５２０６は、切換スイッチ５２４２の接点Ｐａを介して復号処理部５２２２より与えられるセッションキーＫｓ１によって、切換スイッチ５２４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ８および禁止クラスリストの更新日時ＣＲＬｄａｔｅを１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ１をバスＢＳ３に出力する（ステップＳ１３６）。

【０１６３】バスＢＳ３に出力された暗号化データ｛Ｋｓ２／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ１は、バスＢＳ３からインタフェース５２２４および端子５２２６を介してパーソナルコンピュータ５０に出力され、パーソナルコンピュータ５０から配信サーバ１０に送信される（ステップＳ１３８）。

【０１６４】配信サーバ１０は、トランザクションＩＤ／／｛Ｋｓ２／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ１を受信して、復号処理部３２０においてセッションキ

ーＫｓ１による復号処理を実行し、ライセンス管理デバイス５２０で生成されたセッションキーＫｓ２、ライセンス管理デバイス５２０に固有の公開暗号鍵ＫＰｍｃ８およびライセンス管理デバイス５２０における禁止クラスリストＣＲＬの更新日時ＣＲＬｄａｔｅを受理する（ステップＳ１４２）。

【０１６５】配信制御部３１５は、ステップＳ１１０で取得したコンテンツＩＤおよびライセンス購入条件のデータＡＣに従って、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐを生成する（ステップＳ１４４）。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Ｋｃを情報データベース３０４より取得する（ステップＳ１４６）。

【０１６６】配信制御部３１５は、生成したライセンス、すなわち、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、およびアクセス制御情報ＡＣｍを暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたライセンス管理デバイス５２０に固有の公開暗号鍵ＫＰｍｃ８によってライセンスを暗号化して暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８を生成する（ステップＳ１４８）。

【０１６７】図１２を参照して、配信サーバ１０において、ライセンス管理デバイス５２０から送信された禁止クラスリストの更新日時ＣＲＬｄａｔｅが、ＣＲＬデータベース３０６に保持される配信サーバ１０の禁止クラスリストＣＲＬの更新日時と比較されることによってライセンス管理デバイス５２０が保持する禁止クラスリストＣＲＬが最新か否かが判断され、ライセンス管理デバイス５２０が保持する禁止クラスリストＣＲＬが最新と判断されたとき、ステップＳ１５２へ移行する。また、ライセンス管理デバイス５２０が保持する禁止クラスリストＣＲＬが最新でないときはステップＳ１６０へ移行する（ステップＳ１５０）。

【０１６８】最新と判断されたとき、暗号化処理部３２８は、暗号化処理部３２６から出力された暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８をライセンス管理デバイス５２０において発生されたセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２をバスＢＳ１に出力する。そして、配信制御部３１５は、バスＢＳ１上の暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を通信装置３５０を介してパーソナルコンピュータ５０へ送信する（ステップＳ１５２）。

【０１６９】そして、パーソナルコンピュータ５０のコントローラ５１０は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を受信し（ステップＳ１５４）、バスＢＳ５を介してライセンス管理デバイス５２０に入力する。ライセンス管理デバイス５２０の復号処理部５２１２は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を端子５２２６およびインタフェース５２２４を介して受取り、セッションキー発生部５２１８によって発生されたセッションキーＫｓ２によって復号し、｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８を受理する（ステップＳ１５８）。その後、ステップＳ１７２へ移行する。

【０１７０】一方、配信サーバ１０において、ライセンス管理デバイス５２０が保持する禁止クラスリストＣＲＬが最新でないと判断されると、配信制御部３１５は、バスＢＳ１を介してＣＲＬデータベース３０６から最新の禁止クラスリストＣＲＬを取得し、差分データである差分ＣＲＬを生成する（ステップＳ１６０）。

【０１７１】暗号化処理部３２８は、暗号化処理部３２６の出力と、配信制御部３１５がバスＢＳ１を介して供給する禁止クラスリストの差分ＣＲＬとを受けて、ライセンス管理デバイス５２０において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部３２８より出力された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２は、バスＢＳ１および通信装置３５０を介してパーソナルコンピュータ５０に送信される（ステップＳ１６２）。

【０１７２】パーソナルコンピュータ５０は、送信された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を受信し（ステップＳ１６４）、バスＢＳ５を介してライセンス管理デバイス５２０に入力する（ステップＳ１６６）。ライセンス管理デバイス５２０においては、端子５２２６およびインタフェース５２２４を介して、バスＢＳ５に与えられた受信データを復号処理部５２１２によって復号する。復号処理部５２１２は、セッションキー発生部５２１８から与えられたセッションキーＫｓ２を用いてバスＢＳ５の受信データを復号しバスＢＳ５に出力する（ステップＳ１６８）。

【０１７３】この段階で、バスＢＳ５には、Ｋｍｃ保持部５２２１に保持される秘密復号鍵Ｋｍｃ８で復号可能な暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝と、差分ＣＲＬとが出力される（ステップＳ１６８）。コントローラ５２２０の指示によって受理した差分ＣＲＬによってメモリ５２１５内のＣＲＬ領域５２１５Ａを差分ＣＲＬに基づいて更新する（ステップＳ１７０）。

【０１７４】ステップＳ１５２，Ｓ１５４，Ｓ１５６，Ｓ１５８は、ライセンス管理デバイス５２０の禁止クラ

スリストＣＲＬが最新の場合のライセンスのライセンス管理デバイス５２０への配信動作であり、ステップＳ１６０，Ｓ１６２，Ｓ１６４，Ｓ１６６，Ｓ１６８，Ｓ１７０は、ライセンス管理デバイス５２０の禁止クラスリストＣＲＬが最新でない場合のライセンスのライセンス管理デバイス５２０への配信動作である。このように、ライセンス管理デバイス５２０から送られてきた禁止クラスリストの更新日時ＣＲＬｄａｔｅによって、配信を求めてきたライセンス管理デバイス５２０の禁止クラスリストＣＲＬが最新か否かを、逐一、確認し、最新でないとき、最新の禁止クラスリストＣＲＬをＣＲＬデータベース３０６から取得し、差分ＣＲＬをライセンス管理デバイス５２０に配信することによって、ライセンスの破られたライセンス管理デバイスへのライセンスの配信を防止できる。

【０１７５】ステップＳ１５８またはステップＳ１７０の後、コントローラ５２２０の指示によって、暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８は、復号処理部５２０４において、個別秘密復号鍵Ｋｍｃ８によって復号され、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）が受理される（ステップＳ１７２）。

【０１７６】図１３を参照して、コントローラ５１０は、ライセンス管理デバイス５２０が受理したライセンスを格納するエントリを指示するためのエントリ番号を、ライセンス管理デバイス５２０に入力する（ステップＳ１７４）。そうすると、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６およびインタフェース５２２４を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ５２１５のライセンス領域５２１５Ｂに、ステップＳ１７２において取得したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）を格納する（ステップＳ１７６）。

【０１７７】パーソナルコンピュータ５０のコントローラ５１０は、配信サーバ１０から送られたトランザクションＩＤと、暗号化コンテンツデータの配信要求を配信サーバ１０へ送信する（ステップＳ１７８）。

【０１７８】配信サーバ１０は、トランザクションＩＤおよび暗号化コンテンツデータの配信要求を受信し（ステップＳ１８０）、情報データベース３０４より、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する（ステップＳ１８２）。

【０１７９】パーソナルコンピュータ５０は、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理する（ステップＳ１８４）。そうすると、コントローラ５１０は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを１つのコンテンツファイルとしてバスＢＳ２を介してハードディスク（ＨＤＤ）５３０に記録する（ステップＳ１８６）。また、コントローラ５１０は、ライセンス管理デバイス５２０に格納されたライセンスのエントリ番号と、平文のトランザクションＩＤおよびコンテンツＩＤを含む暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、バスＢＳ２を介してＨＤＤ５３０に記録する（ステップＳ１８８）。さらに、コントローラ５１０は、ＨＤＤ５３０に記録されているコンテンツリストファイルに受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や、付加情報Ｄｃ－ｉｎｆから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記し（ステップＳ１９０）、トランザクションＩＤと配信受理を配信サーバ１０へ送信する（ステップＳ１９２）。

【０１８０】配信サーバ１０は、トランザクションＩＤ／／配信受理を受信すると（ステップＳ１９４）、課金データベース３０２への課金データの格納、およびトランザクションＩＤの配信記録データベース３０８への記録が行われて配信終了の処理が実行され（ステップＳ１９６）、全体の処理が終了する（ステップＳ１９８）。

【０１８１】このようにして、パーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５０が正規の認証データを保持する機器であること、同時に、クラス証明書Ｃｍ７とともに暗号化して送信できた公開暗号鍵ＫＰｍ７が有効であることを確認した上で、クラス証明書Ｃｍ７が禁止クラスリスト、すなわち、公開暗号鍵ＫＰｍ７による暗号化が破られたクラス証明書リストに記載されていないライセンス管理デバイスからの配信要求に対してのみコンテンツデータを配信することができ、不正なライセンス管理デバイスへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【０１８２】さらに、配信サーバおよびライセンス管理モジュールでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０１８３】また、ライセンス管理デバイス５２０は、配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信する際に、配信サーバ１０との間でハード的にデータのやり取りを行ない、暗号化コンテンツデータを再生するためのライセンスをハード的に格納するため、そのセキュリティレベルは高い。したがって、ライ

センス管理デバイス５２０を用いれば、パーソナルコンピュータ５０は、セキュリティレベルの高い配信によって暗号化コンテンツデータおよびライセンスを受信できるとともに、セキュリティレベルの高いレベル２ライセンスの管理が可能である。

【０１８４】図１０～１３に示すフローチャートに従って、図１に示す携帯電話機１００に装着されたメモリカード１１０に暗号化コンテンツデータおよびライセンスを携帯電話網を介して配信することも可能である。すなわち、上記の説明において、パーソナルコンピュータ５０を携帯電話機１００に代え、ライセンス管理デバイス５２０をメモリカード１１０に代えれば良い。この場合、図１３に示すステップＳ１８６，Ｓ１８８，Ｓ１９０においては、コンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、および付加情報Ｄｃ－ｉｎｆ）、ライセンス管理ファイル、およびコンテンツリストファイルに代わる再生リストファイルがメモリカード１１０のメモリ１４１５のデータ領域１４１５Ｃに記録される。その他は、上述したのと同じである。

【０１８５】メモリカード１１０への暗号化コンテンツデータおよびライセンスの配信においても暗号化コンテンツデータおよびライセンスをハード的に受信し、かつ、格納するので、メモリカード１１０への暗号化コンテンツデータおよびライセンスの配信は、ライセンス管理デバイス５２０への暗号化コンテンツデータおよびライセンスの配信と同じようにセキュリティレベルの高いレベル２ライセンスの管理が可能である。

【０１８６】［配信２］次に、図１および図２に示すデータ配信システムにおいて、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理モジュール５１１へ暗号化コンテンツデータおよびライセンスを配信する動作について説明する。なお、この動作を「配信２」という。

【０１８７】図１４における処理以前に、パーソナルコンピュータ５０のユーザは、配信サーバ１０に対してモデム４０を介して接続し、購入を希望するコンテンツに対するコンテンツＩＤを取得していることを前提としている。

【０１８８】図１４～図１７は、図１および図２に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生するパーソナルコンピュータ５０に内蔵されたライセンス管理モジュール５１１への配信動作を説明するための第１～第４のフローチャートである。なお、ライセンス管理モジュール５１１は、暗号化コンテンツデータおよびライセンスの配信サーバ１０からの受信をプログラムによって実行する。また、「配信２」における通信路（配信サーバ１０とパーソナルコンピュータ５０間）で交換されるデータの形式およびセキュリティの構成については「配信１」と同様であるが、配信サーバは、２つの公開認証鍵ＫＰａとＫＰｂを用いる。ＫＰａはセキュリティレベルがレベル２であるメモカード１１０およびライセンス管理デバイス５２０の認証データを確認する公開認証鍵であり、ＫＰｂはセキュリティレベルがレベル１であるライセンス管理モジュール５１１の認証データを確認する公開認証鍵である。また、ライセンス管理モジュール５１１はライセンス管理デバイス５２０とほぼ同一の構成を持つソフトウェアモジュールである。ライセンス管理モジュール５１１のクラスを表す自然数ｗはｗ＝５であり、ライセンス管理モジュール５１１を識別するための自然数ｘはｘ＝６であるとする。したがって、ライセンス管理モジュール５１１は、認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰｂ、個別公開暗号鍵ＫＰｍ６、クラス秘密復号鍵Ｋｍ５、個別秘密復号鍵Ｋｍｃ６を保持する。

【０１８９】図１４を参照して、パーソナルコンピュータ５０のユーザからキーボード５６０を介してコンテンツＩＤの指定による配信リクエストがなされる（ステップＳ２００）。そして、キーボード５６０を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣが入力される（ステップＳ２０２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータのアクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐを設定して購入条件ＡＣが入力される。

【０１９０】暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ５１０は、ライセンス管理モジュール５１１から認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰｂを読出し、その読出した認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰｂに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣ、および配信リクエストを配信サーバ１０に対して送信する（ステップＳ２０４）。

【０１９１】配信サーバ１０では、パーソナルコンピュータ５０から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰｂ、およびライセンス購入条件のデータＡＣを受信する（ステップＳ２０６）。そして、配信制御部３１５は、認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰｂのクラス証明書Ｃｍ５に基づいてレベル１の配信を要求しているのか、レベル２の配信を要求しているのかを判別する。認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰｂは、レベル１の配信を要求するライセンス管理モジュール５１１からの認証データであるので、配信制御部３１５はレベル１の配信要求であることを認識する。受信された認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰｂは、復号処理部３１２においてレベル１向けの公開認証鍵ＫＰｂで復号される（ステップＳ２０８）。

【０１９２】配信制御部３１５は、配信制御部３１５は、復号処理部３１２における復号処理結果から、認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰｂがレベル１対応と

して正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ２１０）。正当なレベル１認証データであると判断された場合、配信制御部３１５は、公開暗号鍵ＫＰｍ５および証明書Ｃｍ５を承認し、受理する。そして、ステップＳ２１２へ移行する。また、配信制御部３１５は、正当なレベル１向け認証データでないと判断した場合には、非承認とし、公開暗号鍵ＫＰｍ５および証明書Ｃｍ５を受理しないで処理を終了する（ステップＳ２８８）。

【０１９３】ここでは、これ以上詳細に説明は行わないが、配信サーバ１０はレベル１ライセンスをセキュリティレベルがレベル２であるライセンス管理デバイス５２０やメモリカード１１０へ、パーソナルコンピュータ５０を介して、直接、送信することも可能である。

【０１９４】認証の結果、公開暗号鍵ＫＰｍ５および証明書Ｃｍ５が受理されると、配信制御部３１５は、次に、ライセンス管理モジュール５１１のクラス証明書Ｃｍ５が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ２８８）。

【０１９５】一方、ライセンス管理モジュール５１１のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ２１４）。

【０１９６】認証の結果、公開暗号鍵ＫＰｍ５および証明書Ｃｍ５が受理され、クラス証明書が禁止クラスリストの対象外であることが確認されると、配信サーバ１０において、配信制御部３１５は、配信を特定するための管理コードであるトランザクションＩＤを生成する（ステップＳ２１４）。また、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ２１６）。セッションキーＫｓ１は、復号処理部３１２によって得られたライセンス管理モジュール５１１に対応するクラス公開暗号鍵ＫＰｍ５によって、暗号化処理部３１８によって暗号化される（ステップＳ２１８）。

【０１９７】トランザクションＩＤおよび暗号化されたセッションキーＫｓ１は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ５として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ２２０）。

【０１９８】図１５を参照して、パーソナルコンピュータ５０のコントローラ５１０が、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ５を受信すると（ステップＳ２２２）、ライセンス管理モジュール５１１は、｛Ｋｓ１｝Ｋｍ５を受けて、ライセンス管理モジュール５１１に固有なクラス秘密復号鍵Ｋｍ５によって復号処理を行ない、セッションキーＫｓ１を受理する（ステップＳ２２４）。

【０１９９】ライセンス管理モジュール５１１は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキーＫｓ２を生成する（ステップＳ２２６）。そして、コントローラ５１０は、バスＢＳ２を介してＨＤＤ５３０に記憶された暗号化ＣＲＬを読出し、ライセンス管理モジュール５１１は、暗号化ＣＲＬを復号して禁止クラスリストＣＲＬを取得し、復号した禁止クラスリストＣＲＬから禁止クラスリストの更新日時ＣＲＬｄａｔｅを取得する（ステップＳ２２８）。ライセンス管理モジュール５１１は、さらに、配信サーバ１０において発生されたセッションキーＫｓ１によって、ライセンス管理モジュール５１１で発生させたセッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ６および禁止クラスリストの更新日時ＣＲＬｄａｔｅを１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍｃ６／／ＣＲＬｄａｔｅ｝Ｋｓ１を出力する（ステップＳ２３０）。

【０２００】コントローラ５１０は、暗号化データ｛Ｋｓ２／／ＫＰｍｃ６／／ＣＲＬｄａｔｅ｝Ｋｓ１にトランザクションＩＤを加えたトランザクションＩＤ／／｛Ｋｓ２／／ＫＰｍｃ６／／ＣＲＬｄａｔｅ｝Ｋｓ１を配信サーバ１０へ送信する（ステップＳ２３２）。

【０２０１】配信サーバ１０は、トランザクションＩＤ／／｛Ｋｓ２／／ＫＰｍｃ６／／ＣＲＬｄａｔｅ｝Ｋｓ１を受信して（ステップＳ２３４）、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、ライセンス管理モジュール５１１で生成されたセッションキーＫｓ２、ライセンス管理モジュール５１１に固有な個別公開暗号鍵ＫＰｍｃ６およびライセンス管理モジュール５１１における禁止クラスリストの更新日時ＣＲＬｄａｔｅを受理する（ステップＳ２３６）。

【０２０２】配信制御部３１５は、ステップＳ２０６で取得したコンテンツＩＤおよびライセンス購入条件のデータＡＣに従って、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐを生成する（ステップＳ２３８）。さらに、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号するためのライセンス鍵Ｋｃを情報データベース３０４より取得する（ステップＳ２４０）。

【０２０３】配信制御部３１５は、生成したライセンス、すなわち、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、およびアクセス制御情報ＡＣｍを暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたライセンス管理モジュール５１１に固有な公開暗号鍵ＫＰｍｃ６によってライセンスを暗号化して暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６を生成する（ステップＳ２４２）。

【０２０４】図１６を参照して、配信サーバ１０において、ライセンス管理モジュール５１１から送信された禁

止クラスリストの更新日時ＣＲＬｄａｔｅが、ＣＲＬデータベース３０６に保持される配信サーバ１０の禁止クラスリストＣＲＬの更新日時と比較することによってライセンス管理モジュール５１１が保持する禁止クラスリストＣＲＬが最新か否かが判断され、ライセンス管理モジュール５１１が保持する禁止クラスリストＣＲＬが最新と判断されたとき、ステップＳ２４６へ移行する。また、ライセンス管理モジュール５１１が保持する禁止クラスリストＣＲＬが最新でないときはステップＳ２５２へ移行する（ステップＳ２４４）。

【０２０５】最新と判断されたとき、暗号化処理部３２８は、暗号化処理部３２６から出力された暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６をライセンス管理モジュール５１１において発生されたセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２をバスＢＳ１に出力する。そして、配信制御部３１５は、バスＢＳ１上の暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２を通信装置３５０を介してパーソナルコンピュータ５０へ送信する（ステップＳ２４６）。

【０２０６】そして、パーソナルコンピュータ５０のコントローラ５１０は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２を受信し（ステップＳ２４８）、ライセンス管理モジュール５１１は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２をセッションキーＫｓ２によって復号し、｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６を受理する（ステップＳ２５０）。その後、ステップＳ１６２へ移行する。

【０２０７】一方、配信サーバ１０において、ライセンス管理モジュール５１１が保持する禁止クラスリストＣＲＬが最新でないと判断されると、配信制御部３１５は、バスＢＳ１を介してＣＲＬデータベース３０６から最新の禁止クラスリストＣＲＬを取得し、差分データである差分ＣＲＬを生成する（ステップＳ２５２）。

【０２０８】暗号化処理部３２８は、暗号化処理部３２６の出力と、配信制御部３１５がバスＢＳ１を介して供給する禁止クラスリストの差分ＣＲＬとを受けて、ライセンス管理モジュール５１１において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部３２８より出力された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２は、バスＢＳ１および通信装置３５０を介してパーソナルコンピュータ５０に送信される（ステップＳ２５４）。

【０２０９】パーソナルコンピュータ５０は、送信された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２を受信し（ステップＳ２５６）、ライセンス管理モジュール５１１は、セッションキーＫｓ２を用いて受信データを復号して差分ＣＲＬと暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６とを受理する（ステップＳ２５８）。

【０２１０】コントローラ５１０は、ＨＤＤ５３０に記録された禁止クラスリストＣＲＬに受理した差分ＣＲＬを加え、独自の暗号処理を施し、ＨＤＤ５３０内の禁止クラスリストＣＲＬを書換える（ステップＳ２６０）。

【０２１１】ステップＳ２４６，Ｓ２４８，Ｓ２５０は、ライセンス管理モジュール５１１の禁止クラスリストＣＲＬが最新の場合のライセンス鍵Ｋｃ等のライセンス管理モジュール５１１への配信動作であり、ステップＳ２５２，Ｓ２５４，Ｓ２５６，Ｓ２５８，Ｓ２６０は、ライセンス管理モジュール５１１の禁止クラスリストＣＲＬが最新でない場合のライセンス鍵Ｋｃ等のライセンス管理モジュール５１１への配信動作である。このように、ライセンス管理モジュール５１１から送られてきた禁止クラスリストＣＲＬｄａｔｅが更新されているか否かを、逐一、確認し、更新されていないとき、最新の禁止クラスリストＣＲＬｄａｔｅをＣＲＬデータベース３０６から取得し、差分ＣＲＬをライセンス管理モジュール５１１に配信することによって、ライセンスの破られたライセンス管理モジュールへの暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの配信を防止できる。

【０２１２】ステップＳ２５０またはステップＳ２６０の後、暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６は、秘密復号鍵Ｋｍｃ６によって復号され、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）が受理される（ステップＳ２６２）。

【０２１３】図１７を参照して、ライセンス管理モジュール５１１は、配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスを他の装置へ貸出すためのチェックアウト可能数を含むチェックアウト情報を生成する（ステップＳ２６４）。この場合、チェックアウトの初期値は「３」に設定される。そうすると、ライセンス管理モジュール５１１は、受理したライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐ）と、生成したチェックアウト情報とに独自の暗号処理を施した暗号化レベル１拡張ライセンスを生成する（ステップＳ２６６）。この場合、ライセンス管理モジュール５１１は、パーソナルコンピュータ５０のコントローラ（ＣＰＵ）５１０の識別番号等に基づいて暗号化

を行なう。したがって、生成された暗号化レベル拡張１ライセンスは、パーソナルコンピュータ５０に独自なライセンスになり、後述するチェックアウトを用いなければ、暗号化コンテンツデータおよびライセンスを他の装置へ通信することはできない。セキュリティレベルがレベル１の管理においてのライセンスの移動は、セキュリティホールが明らかに存在するために、ライセンスの移動が許されていないためである。

【０２１４】パーソナルコンピュータ５０のコントローラ５１０は、配信サーバ１０から送られたトランザクションＩＤと、暗号化コンテンツデータの配信要求を配信サーバ１０へ送信する（ステップＳ２６８）。

【０２１５】配信サーバ１０は、トランザクションＩＤおよび暗号化コンテンツデータの配信要求を受信し（ステップＳ２７０）、情報データベース３０４より、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する（ステップＳ２７２）。

【０２１６】パーソナルコンピュータ５０は、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理する（ステップＳ２７４）。そうすると、コントローラ５１０は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを１つのコンテンツファイルとしてバスＢＳ２を介してハードディスク（ＨＤＤ）５３０に記録する（ステップＳ２７６）。また、コントローラ５１０は、ライセンス管理モジュール５１１によって生成された暗号化レベル１拡張ライセンスと、平文のトランザクションＩＤおよびコンテンツＩＤを含む暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、バスＢＳ２を介してＨＤＤ５３０に記録する（ステップＳ２７８）。さらに、コントローラ５１０は、ＨＤＤ５３０に記録されているコンテンツリストファイルに受理したコンテンツの情報として、記録したコンテンツファイルおよびライセンス管理ファイルの名称や、付加情報Ｄｃ－ｉｎｆから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）を追記し（ステップＳ２８０）、トランザクションＩＤと配信受理を配信サーバ１０へ送信する（ステップＳ２８２）。

【０２１７】配信サーバ１０は、トランザクションＩＤ／／配信受理を受信すると（ステップＳ２８４）、課金データベース３０２への課金データの格納、およびトランザクションＩＤの配信記録データベース３０８への記録が行なわれて配信終了の処理が実行され（ステップＳ２８６）、全体の処理が終了する（ステップＳ２８８）。

【０２１８】このように、配信サーバおよびライセンス管理モジュールでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができること、および禁止クラスリストＣＲＬの運用を行なっている点においてライセンス管理デバイス５２０およびメモリカード１１０にライセンスを直接配信する場合と同様である。

【０２１９】しかしながら、パーソナルコンピュータ５０内において、ライセンス管理モジュール５１１は、ソフトウェアにてデータのやり取りを行ない、ライセンスを配信サーバ１０から受信し、管理する点においてライセンス管理モジュール５１１によるライセンスの配信は、ライセンス管理デバイス５２０およびメモリカード１１０に、ライセンスを、直接、配信するよりもセキュリティレベルは低い。

【０２２０】［移動］図１および図２に示すデータ配信システムにおいて、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理デバイス５２０へ配信された暗号化コンテンツデータおよびライセンスを携帯電話機１００または再生端末１０２に装着されたメモリカード１１０へ送信する動作について説明する。なお、この動作を「移動」といい、セキュリティレベルがレベル２間でのみ行われる処理である。

【０２２１】図１８～図２１は、図１および図２に示すデータ配信システムにおいて、ライセンス管理デバイス５２０が配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスを携帯電話機１００または再生端末１０２に装着されたメモリカード１１０へ移動する移動動作を説明するための第１～第４のフローチャートである。携帯電話機１００または再生端末１０２は、移動においては、データの中継を行なうのみの機器であるため、フローチャートから省略してある。移動を説明するに当たり、図２の再生端末１０２に装着されたメモリカード１１０へ移動する場合について説明を行なうが、図１の携帯電話機１００に装着されたメモリカード１１０へ移動する場合についても同様であり、再生端末１０２を携帯電話機１００に読替えれば良い。

【０２２２】なお、図１８における処理以前に、パーソナルコンピュータ５０のユーザは、コンテンツリストファイルに従って、移動するコンテンツを決定し、コンテンツファイルおよびライセンス管理ファイルが特定できていることを前提として説明する。

【０２２３】図１８を参照して、パーソナルコンピュータ５０のキーボード５６０から移動リクエストが入力されると（ステップＳ３００）、コントローラ５１０は、認証データの送信要求をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信する（ステップＳ３０２）。そうすると、再生端末１０２のコントローラ１１０６は、端子１

１１４、ＵＳＢインタフェース１１１２およびバスＢＳ３を介して認証データの送信要求を受信し、バスＢＳ３およびメモリカードインタフェース１２００を介して認証データの送信要求をメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ３０４）。

【０２２４】コントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１０２へ出力する。そして、再生端末１０２のコントローラ１１０６は、メモリカードインタフェース１２００およびバスＢＳ３を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受取り、バスＢＳ３、ＵＳＢインタフェース１１１２、端子１１１４およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを送信する（ステップＳ３０６）。

【０２２５】そうすると、パーソナルコンピュータ５０のコントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受信し（ステップＳ３０８）、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ２を介してライセンス管理デバイス５２０へ送信する。ライセンス管理デバイス５２０のコントローラ５２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受信し、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを復号処理部５２０８へ与える。認証処理部５２０８は、ＫＰａ保持部５２１４からの認証鍵ＫＰａによって認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａの復号処理を実行する（ステップＳ３１０）。コントローラ５２２０は、復号処理部５２０８における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからのクラス公開暗号鍵ＫＰｍ３とクラス証明書Ｃｍ３とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ３１２）。正当な認証データであると判断された場合、コントローラ５２２０は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ３１４）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ４０４）。

【０２２６】ここで、ライセンス管理デバイス５２０はレベル２対応の公開認証鍵ＫＰａしか保持しないため、仮に、セキュリティレベルがレベル１であるライセンス管理モジュール５１１からの要求である場合には、認証に失敗し、処理は終了するため、レベル２からレベル１への移動は行なえない。

【０２２７】認証の結果、正規のメモリカードであることが認識されると、コントローラ５２２０は、次に、メモリカード１１０のクラス証明書Ｃｍ３が禁止クラスリストＣＲＬにリストアップされているかどうかをメモリ５２１５のＣＲＬ領域５２１５Ａに照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで移動動作を終了する（ステップＳ４０４）。

【０２２８】一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ３１４）。

【０２２９】認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理デバイス５２０において、コントローラ５２２０は、管理コードであるトランザクションＩＤをメモリ５２１５のライセンス領域５２１５Ｂから取得する（ステップＳ３１６）。そして、セッションキー発生部５２１８は、移動のためのセッションキーＫｓ２２を生成する（ステップＳ３１８）。セッションキーＫｓ２２は、復号処理部５２０８によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ３によって、暗号化処理部５２１０によって暗号化される（ステップＳ３２０）。コントローラ５２２０は、バスＢＳ５を介して暗号化データ｛Ｋｓ２２｝Ｋｍ３を取得し、メモリ５２１５から取得したトランザクションＩＤを暗号化データ｛Ｋｓ２２｝Ｋｍ３に追加したトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３をバスＢＳ５、インタフェース５２２４および端子５２２６を介して出力する（ステップＳ３２２）。

【０２３０】図１９を参照して、パーソナルコンピュータ５０のコントローラ５１０は、バスＢＳ２を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信し（ステップＳ３２４）、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を再生端末１０２へ送信する（ステップＳ３２４）。そうすると、再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信し、その受信したトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３をメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介してトラ

ンザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信する（ステップＳ３２６）。復号処理部１４２２は、コントローラ１４２０からバスＢＳ４を介して｛Ｋｓ２２｝Ｋｍ３を受取り、Ｋｍ保持部１４２１からのクラス秘密復号鍵Ｋｍ３によって｛Ｋｓ２２｝Ｋｍ３を復号してセッションキーＫｓ２２を受理する（ステップＳ３２８）。そして、セッションキー発生部１４１８は、セッションキーＫｓ２を生成し（ステップＳ３３０）、コントローラ１４２０は、バスＢＳ４を介してメモリ１４１５のＣＲＬ領域１４１５Ａから禁止クラスリストの更新日時ＣＲＬｄａｔｅを取得し、その取得した更新日時ＣＲＬｄａｔｅを切換スイッチ１４４６へ与える（ステップＳ３３２）。

【０２３１】そうすると、暗号化処理部１４０６は、切換スイッチ１４４６の端子を順次切換えることによって取得したセッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ４および禁止クラスリストの更新日時ＣＲＬｄａｔｅを、復号処理部１４０４によって復号されたセッションキーＫｓ２２によって暗号化し、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を生成する。コントローラ１４２０は、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２をバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１０２へ出力し、再生端末１０２のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受取る。そして、コントローラ１１０６は、ＵＳＢインタフェース１１１２、端子１１１４、およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ送信する（ステップＳ３３４）。

【０２３２】パーソナルコンピュータ５０のコントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受信し（ステップＳ３３６）、バスＢＳ２を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２をライセンス管理デバイス５２０へ入力する（ステップＳ３３８）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４およびバスＢＳ５を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受信し、その受信した暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を復号処理部５２１２に与える。復号処理部５２１２は、セッションキー発生部５２１８からのセッションキーＫｓ２２によって暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を復号し、セッションキーＫｓ２、公開暗号鍵ＫＰｍｃ４および禁止クラスリストの更新日時ＣＲＬｄａｔｅを受理する（ステップＳ３４０）。

【０２３３】そうすると、パーソナルコンピュータ５０のコントローラ５１０は、ステップＳ３２４においてＨＤＤ５３０に記録されたライセンス管理ファイルに含まれるライセンスのエントリ番号をＨＤＤ５３０から読出す。そして、コントローラ５１０は、その読出したエントリ番号をバスＢＳ２を介してライセンス管理デバイス５２０に入力する（ステップＳ３４２）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介してエントリ番号を受信し、エントリ番号によって指定されるメモリ５２１５のライセンス領域５２１５Ｂのエントリからライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、再生制御情報ＡＣｐ）を読出す（ステップＳ３４４）。

【０２３４】コントローラ５２２０は、次いで、アクセス制御情報ＡＣｍを確認する（ステップＳ３４６）。つまり、コントローラ５２２０は、取得したアクセス制御情報ＡＣｍに基づいて、最初に、再生端末１０２に装着されたメモリカード１１０へ移動しようとするライセンスが再生回数によって暗号化コンテンツデータの再生ができないライセンスになっていないか否かを確認する。再生回数が残っていない場合（再生回数＝０）、暗号化コンテンツデータをライセンスによって再生することができず、その暗号化コンテンツデータとライセンスとを再生端末１０２に装着されたメモリカード１１０へ移動する意味がないからである。再生することができない場合、再生することができる場合、移動・複製フラグによって、ライセンスの複製、移動の可否を判断する。

【０２３５】ステップＳ３４６において、暗号化コンテンツデータの再生回数ができない（再生回数＝０）、または、移動・複製フラグが移動複製禁止（＝０）の場合、アクセス制御情報ＡＣｍによって、複製移動不可と判断し、ステップＳ４０４へ移行し、移動動作は終了する。ステップＳ３４６において、暗号化コンテンツデータの再生ができ（再生回数≠０）、かつ、移動・複製フラグが移動のみ可「＝１」の場合、ライセンスの移動であると判断され、コントローラ５１０は、メモリ５２１５のライセンス領域５２１５Ｂにおいて指定されたエントリ番号内のライセンスを削除し（ステップＳ３４８）、ステップＳ３５０へ移行する。また、暗号化コンテンツデータの再生ができ「再生回数≠０」、かつ、移動・複製フラグが移動複製可「＝３」の場合、ライセンスの複製であると判断され、ステップＳ３４８を行なわずにステップＳ３５０へ移行する。

【０２３６】図２０を参照して、暗号化処理部５２１７は、復号処理部５２１２によって得られたライセンス管理デバイス５２０に固有の公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ３５０）。そし

て、メモリカード１１０から送信された禁止クラスリストの更新日時ＣＲＬｄａｔｅが、ライセンス管理デバイス５２０がＣＲＬ領域５２１５Ａに保持している禁止クラスリストの更新日時と比較され、いずれの禁止クラスリストが新しいかが判断され、メモカード１００の方が新しいと判断されたとき、ステップＳ３５０へ移行する。また、ライセンス管理デバイス５２０の方が新しいと判断されたときはステップＳ３６２へ移行する（ステップＳ３５２）。

【０２３７】メモリカード１１０の方が新しいと判断されたとき、暗号化処理部５２０６は、暗号化処理部５２１７から出力された暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４をセッションキー発生部５２１８において発生されたセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ５に出力する。そして、コントローラ５２２０は、バスＢＳ５上の暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をインタフェース５２２４および端子５２２６を介してパーソナルコンピュータ５０へ送信する（ステップＳ３５４）。

【０２３８】パーソナルコンピュータ５０のコントローラ５１０は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受取り、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信する（ステップＳ３５６）。

【０２３９】再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し、その受信した暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信する（ステップＳ３５８）。

【０２４０】メモリカード１１０の復号処理部１４１２は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって復号し、｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ３６０）。その後、図２１に示すステップＳ３７４へ移行する。

【０２４１】一方、ステップＳ３５０において、ライセンス管理デバイス５２０の方が新しいと判断されると、ライセンス管理デバイス５２０のコントローラ５２２０は、バスＢＳ５を介してメモリ５２１５のＣＲＬ領域５２１５Ａから最新の禁止クラスリストのデータＣＲＬを取得する（ステップＳ３６２）。

【０２４２】暗号化処理部５２０６は、暗号化処理部５２１７の出力と、コントローラ５２２０がバスＢＳ５を介してメモリ５２１５から取得した禁止クラスリストのデータＣＲＬとを、それぞれ、切換スイッチ５２４２および５２４６を介して受取り、セッションキー発生部５２１８において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部５２０６より出力された暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２は、バスＢＳ５、インタフェース５２２４、および端子５２２６を介してパーソナルコンピュータ５０に出力される（ステップＳ３６４）。

【０２４３】パーソナルコンピュータ５０のコントローラ５１０は、出力された暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を再生端末１０２へ送信する（ステップＳ３６６）。再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受取り、バスＢＳ３およびメモリカードインタフェース１２００を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信する（ステップＳ３６８）。

【０２４４】メモリカード１１０において、復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ４上の受信データを復号し、ＣＲＬと｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４とを受理する（ステップ３７０）。コントローラ１４２０は、復号処理部１４１２によって受理されたデータ

ＣＲＬをバスＢＳ４を介して受取り、その受取ったデータＣＲＬによってメモリ１４１５のＣＲＬ領域１４１５Ａを書換える（ステップＳ３７２）。

【０２４５】ステップＳ３５４，Ｓ３５６，Ｓ３５８，Ｓ３６０は、送信側のライセンス管理デバイス５２０の禁止クラスリストＣＲＬより、受信側のメモリカード１１０の禁止クラスリストＣＲＬが新しい場合のライセンス鍵Ｋｃ等のメモリカード１１０への移動動作であり、ステップＳ３６２，Ｓ３６４，Ｓ３６６，Ｓ３６８，Ｓ３７０，Ｓ３７２は、受信側のメモリカード１１０の禁止クラスリストＣＲＬより、送信側のライセンス管理デバイス５２０の禁止クラスリストＣＲＬが新しい場合のライセンス鍵Ｋｃ等のメモリカード１１０への移動動作である。このように、メモリカード１１０から送られてきた更新日時ＣＲＬｄａｔｅによって、逐一、確認し、できる限り最新の禁止クラスリストＣＲＬをメモリカード１１０の禁止クラスリストＣＲＬとしてＣＲＬ領域１５１４Ａに格納させることによって、ライセンスの破られた機器へのライセンスの流出を防止できる。

【０２４６】図２１を参照して、ステップＳ３６０またはステップＳ３７２の後、コントローラ１４２０の指示によって、暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）が受理される（ステップＳ３７４）。

【０２４７】パーソナルコンピュータ５０のコントローラ５１０は、メモリカード１１０へ移動したライセンスを格納するためのエントリ番号を、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信する。そうすると、再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してエントリ番号を受取り、バスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信し、メモリカード１１０のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ｂに、ステップＳ３７４において取得したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）を格納する（ステップＳ３７８）。

【０２４８】パーソナルコンピュータ５０のコントローラ５１０は、メモリカード１１０のメモリ１４１５に格納されたライセンスのエントリ番号と、平文のトランザクションＩＤおよびコンテンツＩＤを含むメモリカード１１０へ移動しようとする暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、メモリカード１１０へ送信する（ステップＳ３８０）。

【０２４９】メモリカード１１０のコントローラ１４２０は、再生端末１０２を介してライセンス管理ファイルを受信し、メモリ１４１５のデータ領域１４１５Ｃに受信したライセンス管理ファイルを記録する（ステップＳ３８２）。

【０２５０】そして、パーソナルコンピュータ５０のコントローラ５１０は、ステップＳ３４６の判断に従って（ステップＳ３４８）、移動であればＨＤＤ５３０に記録されたライセンスのうち、メモリカード１１０へ移動したライセンスに対するライセンス管理ファイルのライセンスエントリ番号を消去し、ライセンス無に更新する（ステップＳ３８６）。その後、コントローラ５１０は、メモリカード１１０へ移動しようとする暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとをＨＤＤ５３０から取得し、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをメモリカード１１０へ送信する（ステップＳ３９０）。メモリカード１１０のコントローラ１４２０は、再生端末１０２を介して｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信し（ステップＳ３９２）、バスＢＳ４を介して受信した｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをコンテンツファイルとしてメモリ１４１５のデータ領域１４１５Ｃに記録する（ステップＳ３９４）。

【０２５１】そうすると、パーソナルコンピュータ５０のコントローラ５１０は、メモリカード１１０へ移動した楽曲を追記した再生リストを作成し（ステップＳ３９６）、再生リストと、再生リストの書換指示とをメモリカード１１０へ送信する（ステップＳ３９８）。メモリカード１１０のコントローラ１４２０は、再生端末１０２を介して再生リストファイルと書換指示とを受信し（ステップＳ４００）、バスＢＳ４を介してメモリ１４１５のデータ領域１４１５Ｃに記録された再生リストファイルを受信した再生リストファイルに書換え（ステップＳ４０２）、移動動作が終了する（ステップＳ４０４）。

【０２５２】このようにして、再生端末１０２に装着されたメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍ３とともに暗号化して送信できた公開暗号鍵ＫＰｍ３が有効であることを確認した上で、クラス証明書Ｃｍ３が禁止クラスリスト、すなわち、公開暗号鍵ＫＰｍ３による暗号化が破られたクラス証明書リストに記載されていないメモリカードへの移動要求に対してのみコンテンツデータを移動することができ、不正なメモリカードへの移動および解読されたクラス鍵を用いた移動を禁止することができる。

【０２５３】また、ライセンス管理デバイスおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その

暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、暗号化コンテンツデータおよびライセンスの移動動作におけるセキュリティを向上させることができる。

【０２５４】また、説明から明らかなように移動処理として説明したが、コンテンツ供給者によって、ライセンスの複製が許可されている場合には、複製処理として実行され、送信側のライセンス管理デバイス５２０にライセンスはそのまま保持される。この場合の複製は、配信時にコンテンツ供給者、すなわち、著作権所有者が複製を許可し、アクセス制御情報ＡＣｍの移動・複製フラグを移動複製可に設定した場合にのみ許可される行為であり、著作権所有者の権利を阻害した行為ではない。アクセス制御情報はライセンスの一部であり、その機密性は保証されているので、著作権は保護されている。

【０２５５】また、この移動動作を用いることによって、配信サーバ１０との通信機能を有さない再生端末１０２のユーザも、パーソナルコンピュータ５０を介して暗号化コンテンツデータおよびライセンスをメモリカードに受信することができ、ユーザの利便性は向上する。

【０２５６】なお、上記においては、パーソナルコンピュータ５０のライセンス管理デバイス５２０からメモリカード１１０へのライセンスの移動について説明したが、メモリカード１１０からライセンス管理デバイス５２０へのライセンスの移動も、図１８～図２１に示すフローチャートに従って行なわれる。つまり、図１において、携帯電話機１００によって配信を受け、メモリカード１１０に格納した暗号化コンテンツデータとライセンスとをパーソナルコンピュータ５０へ退避できることになる。

【０２５７】また、パーソナルコンピュータ５０が配信サーバ１０から受信したライセンスをメモリカード１１０へ移動できるのは、ライセンス管理デバイス５２０が配信サーバ１０からハード的に受信したライセンスだけであり、ライセンス管理モジュール５１１が配信サーバ１０からソフト的に受信した暗号化コンテンツデータおよびライセンスを「移動」という概念によってメモリカードへ送信することはできない。ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０よりも低いセキュリティレベルによってソフト的に配信サーバ１０との間で認証データおよび暗号鍵等のやり取りを行ない、暗号化コンテンツデータおよびライセンスを受信するので、その受信動作において暗号化が破られる可能性は、ライセンス管理デバイス５２０によって暗号化コンテンツデータおよびライセンスを受信する場合よりも高い。したがって、低いセキュリティレベルによって受信し、かつ、管理された暗号化コンテンツデータおよびライセンスを、ライセンス管理デバイス５２０と同じセキュリティレベルによって暗号化コンテンツデータおよびライセンスを受信して管理するメモリカード１１０へ「移動」という概念によって自由に移すことができるとすると、メモリカード１１０におけるセキュリティレベルが低下するので、これを防止するためにライセンス管理モジュール５１１によって受信した暗号化コンテンツデータおよびライセンスを「移動」という概念によってメモリカード１１０へ送信できなくしたものである。

【０２５８】しかしながら、ライセンス管理モジュール５１１によって受信されたセキュリティレベルの低い暗号化コンテンツデータおよびライセンスを、一切、メモリカード１１０へ移すことができないとすると、著作権を保護しながらコンテンツデータの自由なコピーを許容するデータ配信システムの趣旨に反し、ユーザの利便性も向上しない。そこで、次に説明するチェックアウトおよびチェックインの概念によってライセンス管理モジュール５１１によって受信した暗号化コンテンツデータおよびライセンスをメモリカード１１０へ送信できるようにした。

【０２５９】［チェックアウト］図１および図２に示すデータ配信システムにおいて、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理モジュール５１１へ配信された暗号化コンテンツデータおよびライセンスを再生端末１０２に装着されたメモリカード１１０に送信する動作について説明する。なお、この動作を「チェックアウト」という。

【０２６０】図２２～図２５は、図１および図２に示すデータ配信システムにおいて、ライセンス管理モジュール５１１が配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスを、返却を条件として再生端末１０２に装着されたメモリカード１１０へ暗号化コンテンツデータおよびライセンスを貸出すチェックアウト動作を説明するための第１～第４のフローチャートである。携帯電話機１００または再生端末１０２は、チェックアウトにおいてもデータの中継を行なうのみの機器であるため、フローチャートから省略してある。説明するに当たり、図２の再生端末１０２に装着されたメモリカード１１０へ移動する場合について説明を行なうが、図１の携帯電話機１００に装着されたメモリカード１１０へ移動する場合についても同様であり、再生端末１０２を携帯電話機１００に読替えれば良い。

【０２６１】なお、図２０における処理以前に、パーソナルコンピュータ５０のユーザは、コンテンツリストファイルに従って、チェックアウトするコンテンツを決定し、コンテンツファイルおよびライセンス管理ファイルが特定できていることを前提として説明する。

【０２６２】図２２を参照して、パーソナルコンピュータ５０のキーボード５６０からチェックアウトリクエストが入力されると（ステップＳ５００）、コントローラ５１０は、ＨＤＤ５３０に記録されたライセンス管理ファイルから暗号化ライセンスデータを取得する。この場

合、ライセンス管理ファイルは、ライセンス管理モジュール５１１によって暗号化コンテンツデータおよびライセンスを受信し、独自の暗号化を施した暗号化レベル１拡張ライセンスを格納したものである（図１７のステップＳ２６６参照）。ライセンス管理モジュール５１１は、チェックアウトしたい暗号化ライセンスデータの暗号化レベル１拡張ライセンスをライセンス管理ファイルから取得し、復号してライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、再生制御情報ＡＣｐ）、およびチェックアウト情報を取得する（ステップＳ５０２）。

【０２６３】ライセンス管理モジュール５１１は、アクセス制御情報ＡＣｍを確認する（ステップＳ５０４）。つまり、ライセンス管理モジュール５１１は、取得したアクセス制御情報ＡＣｍに基づいて、再生端末１０２に装着されたメモリカード１１０へチェックアウトしようとするライセンスがアクセス制御情報ＡＣｍによって暗号化コンテンツデータの再生回数の指定がないか、再生ができないライセンスになっていないか否かを確認する。再生に制限がある場合、暗号化コンテンツデータをチェックアウトしたライセンスによって再生することができず、その暗号化コンテンツデータとライセンスとを再生端末１０２に装着されたメモリカード１１０へチェックアウトする意味がないからである。

【０２６４】ステップＳ５０４において、再生に制限がある場合、ステップＳ５８８へ移行し、チェックアウト動作は終了する。ステップＳ５０４において、再生に対する制限がない場合、ステップＳ５０６へ移行する。そして、ライセンス管理モジュール５１１は、取得したチェックアウト情報に含まれるチェックアウト可能数が「０」よりも大きいか否かを確認する（ステップＳ５０６）。ステップＳ５０６において、チェックアウト可能数が「０」以下であれば、すでにチェックアウトできるライセンスがないので、ステップＳ５８８へ移行し、チェックアウト動作は終了する。ステップＳ５０６において、チェックアウト可能数が「０」よりも大きいとき、ライセンス管理モジュール５１１は、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して認証データの送信要求を送信する（ステップＳ５０８）。再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して認証データの送信要求を受信し、その受信した認証データの送信要求をバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ５１０）。

【０２６５】コントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１０２へ出力する。そして、再生端末１０２のコントローラ１１０６は、メモリカードインタフェース１２００およびバスＢＳ３を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受取り、バスＢＳ３、ＵＳＢインタフェース１１１２、端子１１１４およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを送信する（ステップＳ５１２）。

【０２６６】そうすると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受信し（ステップＳ５１４）、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを認証鍵ＫＰａによって復号する（ステップＳ５１６）。ライセンス管理モジュール５１１は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからのクラス公開暗号鍵ＫＰｍ３とクラス証明書Ｃｍ３とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ５１８）。正当な認証データであると判断された場合、ライセンス管理モジュール５１１は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ５２０）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ５８８）。

【０２６７】ここで、ライセンス管理モジュール５１１はレベル１対応の公開認証鍵ＫＰｂしか保持しないため、セキュリティレベルがレベル１へのチェックアウトしか行なえない。

【０２６８】認証の結果、正規のメモリカードであることが認識されると、ライセンス管理モジュール５１１は、次に、メモリカード１１０のクラス証明書Ｃｍ３が禁止クラスリストＣＲＬにリストアップされているかどうかをＨＤＤ５３０に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここでチェックアウト動作を終了する（ステップＳ５８８）。一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ５２０）。

【０２６９】図２３を参照して、認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理モジュール５１１は、チェックアウトを特定するための管理コードであ

るチェックアウト用トランザクションＩＤを生成する（ステップＳ５２２）。チェックアウト用トランザクションＩＤは、必ず、メモリカード１１０に格納されている全てのトランザクションＩＤと異なる値をとり、かつ、ローカル使用のトランザクションＩＤとして生成する。そして、ライセンス管理モジュール５１１は、チェックアウトのためのセッションキーＫｓ２２を生成し（ステップＳ５２４）、メモリカード１１０から送信されたクラス公開暗号鍵ＫＰｍ３によって、生成したセッションキーＫｓ２２を暗号化する（ステップＳ５２６）。そして、ライセンス管理モジュール５１１は、暗号化データ｛Ｋｓ２２｝Ｋｍ３にチェックアウト用トランザクションＩＤを追加したチェックアウト用トランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信する（ステップＳ５２８）。そうすると、再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してチェックアウト用トランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信し、その受信したチェックアウト用トランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３をメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介してチェックアウト用トランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信する（ステップＳ５３０）。復号処理部１４２２は、コントローラ１４２０からバスＢＳ４を介して｛Ｋｓ２２｝Ｋｍ３を受取り、Ｋｍ保持部１４２１からのクラス秘密復号鍵Ｋｍ３によって｛Ｋｓ２２｝Ｋｍ３を復号してセッションキーＫｓ２２を受理する（ステップＳ５３２）。そして、セッションキー発生部１４１８は、セッションキーＫｓ２を生成し（ステップＳ５３４）、コントローラ１４２０は、バスＢＳ４を介してメモリ１４１５のＣＲＬ領域１４１５Ａから禁止クラスリストの更新日時ＣＲＬｄａｔｅを取得し、その取得した更新日時ＣＲＬｄａｔｅを切換スイッチ１４４６へ与える（ステップＳ５３６）。

【０２７０】そうすると、暗号化処理部１４０６は、切換スイッチ１４４６の端子を順次切換えることによって取得したセッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ４および更新日時ＣＲＬｄａｔｅを、復号処理部１４０４によって復号されたセッションキーＫｓ２２によって暗号化し、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を生成する。コントローラ１４２０は、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２をバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１０２へ出力し、再生端末１０２のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受取る。そして、コントローラ１１０６は、ＵＳＢインタフェース１１１２、端子１１１４、およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ送信する（ステップＳ５３８）。

【０２７１】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受信し（ステップＳ５４０）、その受信した暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２をセッションキーＫｓ２２によって復号し、セッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ４および更新日時ＣＲＬｄａｔｅを受理する（ステップＳ５４２）。そして、ライセンス管理モジュール５１１は、再生端末１０２に装着されたメモリカードから他のメモリカード等へライセンスが移動／複製されないチェックアウト用アクセス制御情報ＡＣｍを生成する。すなわち、再生回数を無制限（＝２５５）、移動・複製フラグを移動複製不可（＝３）にしたアクセス制御情報ＡＣｍを生成する（ステップＳ５４４）。

【０２７２】図２４を参照して、ライセンス管理モジュール５１１は、ステップＳ５４２において受信したライセンス管理モジュール５１１に固有の公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ５４６）。そして、メモリカード１１０から送信された禁止クラスリストの更新日時ＣＲＬｄａｔｅが、ライセンス管理モジュール５１１が管理するＨＤＤ５３０に保持される禁止クラスリストの更新日時と比較され、いずれの禁止クラスリストが新しいかが判断され、メモリカード１１０の方が新しいと判断されたとき、ステップＳ５５０へ移行する。また、逆に、ライセンス管理モジュール５１１の方が新しいときはステップＳ５５６へ移行する（ステップＳ５４８）。

【０２７３】メモリカード１１０の方が新しいと判断されたとき、ライセンス管理モジュール５１１は、暗号化データ｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４をセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信する（ステップＳ５５０）。

【０２７４】再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、お

よびバスＢＳ３を介して暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し、その受信した暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、端子１４２４、およびバスＢＳ４を介して暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信する（ステップＳ５５２）。

【０２７５】メモリカード１１０の復号処理部１４１２は、暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって復号し、｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ５５４）。その後、図２５に示すステップＳ５６６へ移行する。

【０２７６】一方、ステップＳ５４８において、ライセンス管理モジュール５１１の禁止クラスリストの方が新しい判断されると、ライセンス管理モジュール５１１は、ＨＤＤ５３０からライセンス管理モジュールの管理する禁止クラスリストＣＲＬを取得する（ステップＳ５５６）。

【０２７７】そして、ライセンス管理モジュール５１１は、｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４と、ＨＤＤ５３０から取得した禁止クラスリストのデータＣＲＬとをセッションキーＫｓ２によって暗号化し、その暗号化データ｛ＣＲＬ／／｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をＵＳＢインタフェース５５０、端子５８０およびＵＳＢケーブル７０を介して再生端末１０２へ送信する（ステップＳ５５８）。再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛ＣＲＬ／／｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し、その受信した暗号化データ｛ＣＲＬ／／｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ出力する。そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛ＣＲＬ／／｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信する（ステップＳ５６０）。

【０２７８】メモリカード１１０において、復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ４上の受信データを復号し、ＣＲＬと｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４とを受理する（ステップ５６０）。コントローラ１４２０は、復号処理部１４１２によって受理されたデータＣＲＬをバスＢＳ４を介して受取り、その受取ったデータＣＲＬによってメモリ１４１５のＣＲＬ領域１４１５Ａを書換える（ステップＳ５６４）。

【０２７９】ステップＳ５５０，Ｓ５５２，Ｓ５５４は、送信側のライセンス管理モジュール５１１の禁止クラスリストＣＲＬより、受信側のメモリカード１１０の禁止クラスリストＣＲＬが新しい場合のライセンス鍵Ｋｃ等のメモリカード１１０へのチェックアウト動作であり、ステップＳ５５６，Ｓ５５８，Ｓ５６０，Ｓ５６２，Ｓ５６４は、受信側のメモリカード１１０の禁止クラスリストＣＲＬより、送信側のライセンス管理モジュール５１１の禁止クラスリストＣＲＬが新しい場合のライセンス鍵Ｋｃ等のメモリカード１１０へのチェックアウト動作である。このように、メモリカード１１０から送られてきた禁止クラスリストの更新日時ＣＲＬｄａｔｅによって、逐一、確認し、できる限り最新の禁止クラスリストＣＲＬをＨＤＤ５３０から取得し、メモリカード１１０の禁止クラスリストＣＲＬとしてＣＲＬ領域１５１４Ａに格納させることによって、機器へのライセンスの流出を防止できる。

【０２８０】図２５を参照して、ステップＳ５５４またはステップＳ５６４の後、コントローラ１４２０の指示によって、暗号化ライセンス｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、チェックアウト用トランザクションＩＤ、コンテンツＩＤ、チェックアウト用ＡＣｍおよび再生制御情報ＡＣｐ）が受理される（ステップＳ５５６）。

【０２８１】パーソナルコンピュータ５０のコントローラ５１０は、メモリカード１１０へ移動したライセンスを格納するためのエントリ番号を、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信しする（ステップＳ５６

７）。そうすると、再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ｂに、ステップＳ５６６において取得したライセンス（ライセンス鍵Ｋｃ、チェックアウト用トランザクションＩＤ、コンテンツＩＤ、チェックアウト用ＡＣｍおよび再生制御情報ＡＣｐ）を格納する（ステップＳ５６８）。

【０２８２】パーソナルコンピュータ５０のコントローラ５１０は、メモリカード１１０のメモリ１４１５に格納されたライセンスのエントリ番号と、平文のチェックアウト用トランザクションＩＤおよびコンテンツＩＤを含むメモリカード１１０へ移動しようとする暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、メモリカード１１０へ送信する（ステップＳ５６９）。

【０２８３】メモリカード１１０のコントローラ１４２０は、再生端末１０２を介してライセンス管理ファイルを受信し、その受信したライセンス管理ファイルをメモリ１４１５のデータ領域１４１５Ｃに記録する（ステップＳ５７０）。

【０２８４】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、チェックアウト可能数を１減算し（ステップＳ５７１）、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、再生制御情報ＡＣｐ、および更新したチェックアウト情報（チェックアウト可能数と、チェックアウト用トランザクションＩＤと、チェックアウト先のメモリカード１１０の個別公開暗号鍵ＫＰｍｃ４を追加したもの）に独自の暗号を施した新たな暗号化レベル１拡張ライセンスを生成し、その生成した暗号化ライセンスデータによってＨＤＤ５３０に記録されたライセンス管理ファイルのライセンスデータを更新記録する（ステップＳ５７２）。チェックアウト先の個別公開鍵ＫＰｍｃ４は、メモリカードの耐タンパモジュール内に格納され、かつ、認証による暗号を用いたセキュリティの高い通信手段によって入手でき、メモリカードごとに固有値を持つため、メモリカードを特定する識別情報として適している。

【０２８５】ライセンス管理モジュール５１１は、メモリカード１１０へチェックアウトしようとする暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとをＨＤＤ５３０から取得し、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをメモリカード１１０へ送信する（ステップＳ５７４）。メモリカード１１０のコントローラ１４２０は、再生端末１０２を介して｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信し（ステップＳ５７６）、バスＢＳ４を介して受信した｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをコンテンツファイルとしてメモリ１４１５のデータ領域１４１５Ｃに記録する（ステップＳ５７８）。

【０２８６】そうすると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、メモリカード１１０へチェックアウトした楽曲を追記した再生リストを作成し（ステップＳ５８０）、再生リストと、再生リストの書換指示とをメモリカード１１０へ送信する（ステップＳ５８２）。メモリカード１１０のコントローラ１４２０は、再生端末１０２を介して再生リストと書換指示とを受信し（ステップＳ５８４）、バスＢＳ４を介してメモリ１４１５のデータ領域１４１５Ｃに記録されている再生リストファイルを受信した再生リストファイルに書換え（ステップＳ５８６）、チェックアウト動作が終了する（ステップＳ５８８）。

【０２８７】このようにして、再生端末１０２に装着されたメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍ３とともに暗号化して送信できた公開暗号鍵ＫＰｍ３が有効であることを確認した上で、クラス証明書Ｃｍ３が禁止クラスリスト、すなわち、公開暗号鍵ＫＰｍ３による暗号化が破られたクラス証明書リストに記載されていないメモリカードへのチェックアウト要求に対してのみコンテンツデータをチェックアウトすることができ、不正なメモリカードへのチェックアウトおよび解読されたクラス鍵を用いたチェックアウトを禁止することができる。

【０２８８】また、ライセンス管理モジュールおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、暗号化コンテンツデータおよびライセンスのチェックアウト動作におけるセキュリティを向上させることができる。

【０２８９】また、このチェックアウト動作を用いることによって、配信サーバ１０との通信機能を有さない再生端末１０２のユーザも、パーソナルコンピュータ５０がソフト的に受信した暗号化コンテンツデータおよびライセンスをメモリカードに受信することができ、ユーザの利便性は向上する。

【０２９０】［チェックイン］次に、図１および図２に示すデータ配信システムにおいて、パーソナルコンピュータ５０のライセンス管理モジュール５１１からメモリカード１１０へチェックアウトされた暗号化コンテンツデータおよびライセンスをライセンス管理モジュール５１１へ戻す動作について説明する。なお、この動作を「チェックイン」という。

【０２９１】図２６～２８は、図２２～２５を参照して説明したチェックアウト動作によってメモリカード１１０へ貸出された暗号化コンテンツデータおよびライセンスを返却して貰うチェックイン動作を説明するための第１～第３のフローチャートである。携帯電話機１００ま

たは再生端末１０２は、チェックインにおいてもデータの中継を行うのみの機器であるため、フローチャートから省略してある。説明するに当たり、図２の再生端末１０２に装着されたメモリカード１１０から移動する場合について説明を行うが、図１の携帯電話機１００に装着されたメモリカード１１０から移動する場合についても同様であり、再生端末１０２を携帯電話機１００に読み替えれば良い。

【０２９２】なお、図２６における処理以前に、パーソナルコンピュータ５０のユーザは、コンテンツリストファイルに従って、チェックインするコンテンツを決定し、コンテンツファイルおよびライセンス管理ファイルが特定できていることを前提として説明する。

【０２９３】図２６を参照して、パーソナルコンピュータ５０のキーボード５６０からチェックインリクエストが入力されると（ステップＳ６００）、ライセンス管理モジュール５１１は、ＨＤＤ５３０に記録されたライセンス管理ファイルから暗号化レベル１拡張ライセンスデータを取得し、復号してライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、再生制御情報ＡＣｐ）、およびチェックアウト情報（チェックアウト可能数、チェックアウト用トランザクションＩＤ、チェックアウト先のメモリカードの個別公開暗号鍵ＫＰｍｃｘ）を取得する（ステップＳ６０２）。そして、ライセンス管理モジュール５１１は、認証データの送信要求をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信する（ステップＳ６０４）。そうすると、再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２およびバスＢＳ３を介して認証データの送信要求を受信し、バスＢＳ３およびメモリカードインタフェース１２００を介して認証データの送信要求をメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ６０６）。

【０２９４】コントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１０２へ出力する。そして、再生端末１０２のコントローラ１１０６は、メモリカードインタフェース１２００およびバスＢＳ３を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受取り、バスＢＳ３、ＵＳＢインタフェース１１１２、端子１１１４およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを送信する（ステップＳ６０８）。

【０２９５】そうすると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受信し（ステップＳ６１０）、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを認証鍵ＫＰａによって復号する（ステップＳ６１２）。そして、ライセンス管理モジュール５１１は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからのクラス公開暗号鍵ＫＰｍ３とクラス証明書Ｃｍ３とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ６１４）。正当な認証データであると判断された場合、ライセンス管理モジュール５１１は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ６１６）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ６７０）。

【０２９６】認証の結果、正規のメモリカードであることが認識されると、ライセンス管理モジュール５１１は、ダミートランザクションＩＤを生成する（ステップＳ６１６）。ダミー用トランザクションＩＤは、必ず、メモリカード１１０に格納されている全てのトランザクションＩＤと異なる値をとり、かつ、ローカル使用のトランザクションＩＤとして生成される。そして、ライセンス管理モジュール５１１は、チェックイン用のセッションキーＫｓ２２を生成し（ステップＳ６１８）、生成したセッションキーＫｓ２２をメモリカード１１０から受信したクラス公開暗号鍵ＫＰｍ３によって暗号化して暗号化データ｛Ｋｓ２２｝Ｋｍ３を生成し（ステップＳ６２０）、暗号化データ｛Ｋｓ２２｝Ｋｍ３にダミートランザクションＩＤを追加したダミートランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信する（ステップＳ６２２）。

【０２９７】図２７を参照して、再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してダミートランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信し、その受信したダミートランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３をメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介してダミートランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信する（ステップＳ６２４）。復号処理部１４２２は、コントローラ１４２０からバスＢＳ４を介して｛Ｋｓ２２｝Ｋｍ３を受取り、Ｋｍ保持部１４２１からのクラス秘密復

号鍵Ｋｍ３によって｛Ｋｓ２２｝Ｋｍ３を復号してセッションキーＫｓ２２を受理する（ステップＳ６２６）。そして、セッションキー発生部１４１８は、セッションキーＫｓ２を生成し（ステップＳ６２８）、コントローラ１４２０は、バスＢＳ４を介してメモリ１４１５のＣＲＬ領域１４１５Ａから禁止クラスリストＣＲＬの更新日時ｄａｔｅを取得し、その取得した更新日時ＣＲＬｄａｔｅを切換スイッチ１４４６へ与える（ステップＳ６３０）。

【０２９８】そうすると、暗号化処理部１４０６は、切換スイッチ１４４６の端子を順次切換えることによって取得したセッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ４および更新日時ＣＲＬｄａｔｅを、復号処理部１４２２によって復号され、かつ、切換スイッチ１４４２の端子Ｐａを介して取得されたセッションキーＫｓ２２によって暗号化し、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を生成する。コントローラ１４２０は、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２をバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１０２へ出力し、再生端末１０２のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受取る。そして、コントローラ１１０６は、ＵＳＢインタフェース１１１２、端子１１１４、およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ送信する（ステップＳ６３２）。

【０２９９】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受信し（ステップＳ６３４）、その受信した暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２をセッションキーＫｓ２２によって復号し、セッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ４および更新日時ＣＲＬｄａｔｅを受理する（ステップＳ６３６）。

【０３００】そうすると、ライセンス管理モジュール５１１は、受理した個別公開暗号鍵ＫＰｍｃ４がＨＤＤ５３０に記録されたライセンス管理ファイルから取得したチェックアウト情報に含まれる否かを、すなわち、チェックアウトしようとするライセンスのチェックアウト用トランザクションＩＤに対応して格納されている個別公開暗号鍵ＫＰｍｃｘと一致するか否かを確認する（ステップＳ６３８）。この個別公開暗号鍵ＫＰｍｃ４は、暗号化コンテンツデータおよびライセンスのチェックアウトの際に、更新されたチェックアウト情報に含まれるものである（図２５のステップＳ５７２を参照）。したがって、暗号化コンテンツデータ等のチェックアウト先に対応する個別公開暗号鍵ＫＰｍｃ４をチェックアウト情報に含ませることによってチェックインの際にチェックアウトしたチェックアウト先を容易に特定することができる。

【０３０１】ステップＳ６３８において、個別公開暗号鍵ＫＰｍｃ４がチェックアウト情報に含まれていないときチェックイン動作は終了する（ステップＳ６７０）。ステップＳ６３８において、個別公開暗号鍵ＫＰｍｃ４がチェックアウト情報に含まれていると、ライセンス管理モジュール５１１は、ダミートランザクションＩＤを含むダミーライセンス（ダミートランザクションＩＤ、ダミーコンテンツＩＤ、ダミーＫｃ、ダミーＡＣｍ、およびダミーＡＣｐ）を個別公開暗号鍵ＫＰｍｃ４によって暗号化し、暗号化データ｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ６４０）。

【０３０２】ライセンス管理モジュール５１１は、暗号化データ｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４をセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミー鍵Ｋｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を生成し、その生成した暗号化データ｛｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信する（ステップＳ６４２）。

【０３０３】再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーライセンス鍵Ｋｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信する。コントローラ１１０６は、受信した暗号化データ｛｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して｛｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信する（ステップＳ６４４）。

【０３０４】図２８を参照して、メモリカード１１０の復号処理部１４１２は、｛｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって復号し、

｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／Ｋｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ６４６）。そして、復号処理部１４０４は、暗号化データ｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４を復号処理部１４１２から受取り、その受取った暗号化データ｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４をＫｍｃ保持部１４０２からの個別秘密復号鍵Ｋｍｃ４によって復号し、ダミーライセンス（ダミートランザクションＩＤ、ダミーコンテンツＩＤ、ダミーＫｃ、ダミーＡＣｍ、およびダミーＡＣｐ）を受理する（ステップＳ６４８）。

【０３０５】パーソナルコンピュータ５０のコントローラ５１０は、メモリカード１１０のデータ領域１４１５Ｃに記録されているチェックアウトしたライセンスに対応するライセンス管理ファイルからエントリ番号を取得して、ダミーライセンスを格納するためのエントリ番号として、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信する（ステップＳ６４９）。そうすると、再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ｂに、ステップＳ６４８において取得したダミーライセンス（ダミートランザクションＩＤ、ダミーコンテンツＩＤ、ダミーＫｃ、ダミーＡＣｍ、およびダミーＡＣｐ）をメモリ１４１５のライセンス領域１４１５Ｂの指定されたエントリに格納する（ステップＳ６５０）。このようにダミーライセンスをチェックインしたいライセンスに対して上書きすることによってメモリカード１１０へチェックアウトしたライセンスを消去することができる。

【０３０６】その後、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、チェックアウト情報内のチェックアウト可能数を１だけ増やし、チェックアウト用トランザクションＩＤ、およびチェックアウト先のメモリカードの個別公開鍵ＫＰｍｃ４を削除してチェックアウト情報を更新する（ステップＳ６５２）。そして、ライセンス管理モジュール５１１は、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐと更新したチェックアウト情報とに独自の暗号化を施して暗号化ライセンスデータを作成し、ＨＤＤ５３０に記録されたライセンス管理ファイルのライセンスデータを更新記録する（ステップＳ６５４）。

【０３０７】そうすると、ライセンス管理モジュール５１１は、メモリカード１００のメモリ１４１５のデータ領域１４１５Ｃに記録されているチェックアウトしたライセンスに対するコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆ）およびライセンス管理ファイルとを削除する削除指示をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信する（ステップＳ６５６）。再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆ）およびライセンス管理ファイルの削除指示を受信し、バスＢＳ３およびメモリカードインタフェース１２００を介して受信したコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆ）およびライセンス管理ファイルの削除指示をメモリカード１１０へ出力する。そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介してコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆ）およびライセンス管理ファイルの削除指示を受信する（ステップＳ６５８）。そして、コントローラ１４２０は、バスＢＳ４を介してメモリ１４１５のデータ領域１４１５Ｃに記録されたコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆ）およびライセンス管理ファイルを削除する（ステップＳ６６０）。

【０３０８】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、チェックインした楽曲を削除した再生リストを作成し（ステップＳ６６２）、再生リストと、再生リストの書換指示とをメモリカード１１０へ送信する（ステップＳ６６４）。メモリカード１１０のコントローラ１４２０は、再生端末１０２を介して再生リストファイルと書換指示とを受信し（ステップＳ６６６）、バスＢＳ４を介してメモリ１４１５のデータ領域１４１５Ｃの再生リストファイルを受信した再生リストファイルに書換え（ステップＳ６６８）、チェックイン動作が終了する（ステップＳ６７０）。

【０３０９】このように、暗号化コンテンツデータおよびライセンスをチェックアウトした相手先から暗号化コンテンツデータおよびライセンスを返却して貰うことによって、移動が禁止されているセキュリティレベルの低いライセンス管理モジュールからライセンスが、セキュリティレベルの高いメモリカードへ貸出され、メモリカードにおいてセキュリティレベルの低いライセンス管理モジュールで取得したライセンスを受信できるため、再生端末においてセキュリティレベルの低いライセンス管理モジュールで取得したライセンスによって暗号化コンテンツデータを再生して楽しむことができる。

【０３１０】また、メモリカードへ貸出されたライセンスは、アクセス制御情報ＡＣｍによってメモリカードか

ら他の記録機器（メモリカード、ライセンス管理デバイスおよびライセンス管理モジュール）に対して、チェックアウトしたライセンスが出力できないよう指定されているため、貸出したライセンスが流出することはない。貸出したライセンス管理モジュールに対してチェックイン（返却）することで、貸出したライセンスの権利が、貸出したライセンス管理モジュールに戻るようになっている。したがって、著作者の意に反して複製ができることを許すものではなく、セキュリティレベルが低下する処理ではなく、著作権も保護されている。

【０３１１】［再生］次に、図２９および図３０を参照してメモリカード１１０にチェックアウトされたコンテンツデータの再生端末１００（コンテンツ再生デバイスとも言う、以下同じ）における再生動作について説明する。なお、図２９における処理以前に、再生端末１０２のユーザは、メモリカード１００のデータ領域１４１５Ｃに記録されている再生リストに従って、再生するコンテンツ（楽曲）を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

【０３１２】図２９を参照して、再生動作の開始とともに、再生端末１００のユーザから操作パネル１１０８を介して再生指示が再生端末１００にインプットされる（ステップＳ７００）。そうすると、コントローラ１１０６は、バスＢＳ３を介して認証データ保持部１５００から認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを読出し、メモリカードインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを出力する（ステップＳ７０２）。

【０３１３】そうすると、メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを受理する（ステップＳ７０４）。そして、メモリカード１１０の復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを、ＫＰａ保持部１４１４に保持された公開認証鍵ＫＰａによって復号し（ステップＳ７０６）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ７０８）。復号できなかった場合、ステップＳ７４８へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ１４２０は、取得した証明書Ｃｍ１がメモリ１４１５のＣＲＬ領域１４１５Ａから読出した禁止クラスリストＣＲＬに含まれるか否かを判断する（ステップＳ７１０）。この場合、クラス証明書Ｃｐ１には識別番号が付与されており、コントローラ１４２０は、受理したクラス証明書Ｃｐ１の識別番号が禁止クラスリストデータの中に存在するか否かを判別する。クラス証明書Ｃｐ１が禁止クラスリストデータに含まれると判断されると、ステップＳ７４８へ移行し、再生動作は終了する。

【０３１４】ステップＳ７１０において、クラス証明書Ｃｐ１が禁止クラスリストデータＣＲＬに含まれていないと判断されると、メモリカード１１０のセッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ７１２）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をバスＢＳ３へ出力する（ステップＳ７１４）。そうすると、コントローラ１４２０は、インタフェース１４２４および端子１４２６を介してメモリカードインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力する（ステップＳ７１６）。再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得する。そして、Ｋｐ１保持部１５０２は、秘密復号鍵Ｋｐ１を復号処理部１５０４へ出力する。

【０３１５】復号処理部１５０４は、Ｋｐ１保持部１５０２から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１５０６へ出力する（ステップＳ７１８）。そうすると、セッションキー発生部１５０８は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１５０６へ出力する（ステップＳ７２０）。暗号処理部１５０６は、セッションキー発生部１５０８からのセッションキーＫｓ３を復号処理部１５０４からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し、コントローラ１１０６は、バスＢＳ３およびメモリカードインタフェース１２００を介して｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ７２２）。

【０３１６】そうすると、メモリカード１１０の復号処理部１４１２は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して｛Ｋｓ３｝Ｋｓ２を入力する（ステップＳ７２４）。

【０３１７】図３０を参照して、復号処理部１４１２は、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３｝Ｋｓ２を復号して、再生端末１００で発生されたセッションキーＫｓ３を受理する（ステップＳ７２６）。

【０３１８】再生端末のコントローラ１１０６は、メモリカード１１０から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し、メモリカードインタフェース１２００を介してメモリカード１１０へ取得したエントリ番号を出力する（ステップＳ７２７）。

【０３１９】エントリ番号が入力に応じて、コントローラ１４２０は、アクセス制限情報ＡＣｍを確認する（ス

テップＳ７２８）。

【０３２０】ステップＳ７２８においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣｍを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報ＡＣｍの再生回数を更新（１減ずる）した後に次のステップに進む（ステップＳ７３０）。一方、アクセス制限情報ＡＣｍの再生回数によって再生が制限されていない場合においては、ステップＳ７３０はスキップされ、アクセス制限情報ＡＣｍの再生回数は更新されることなく処理が次のステップ（ステップＳ７３２）に進行される。

【０３２１】ステップＳ７２８において、当該再生動作において再生が可能であると判断された場合には、メモリ１４１５のライセンス領域１４１５Ｂに記録された再生リクエスト曲のライセンス鍵Ｋｃおよび再生制御情報ＡＣｐがバスＢＳ４上に出力される（ステップＳ７３２）。

【０３２２】得られたライセンス鍵Ｋｃと再生制御情報ＡＣｐは、切換スイッチ１４４６の接点Ｐｆを介して暗号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐｂを介して復号処理部１４１２より受けたセッションキーＫｓ３によって切換スイッチ１４４６を介して受けたライセンス鍵Ｋｃと再生制御情報ＡＣｐとを暗号化し、｛Ｋｃ／／ＡＣｐ｝Ｋｓ３をバスＢＳ４に出力する（ステップＳ７３４）。

【０３２３】バスＢＳ４に出力された暗号化データは、インタフェース１４２４、端子１４２６、およびメモリカードインタフェース１２００を介して再生端末１００に送出される。

【０３２４】再生端末１００においては、メモリカードインタフェース１２００を介してバスＢＳ３に伝達される暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を復号処理部１５１０によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを受理する（ステップＳ７３６）。復号処理部１５１０は、ライセンス鍵Ｋｃを復号処理部１５１６に伝達し、再生制御情報ＡＣｐをバスＢＳ３に出力する。

【０３２５】コントローラ１１０６は、バスＢＳ３を介して、再生制御情報ＡＣｐを受理して再生の可否の確認を行なう（ステップＳ７４０）。

【０３２６】ステップＳ７４０においては、再生制御情報ＡＣｐによって再生不可と判断される場合には、再生動作は終了される。

【０３２７】ステップＳ７４０において再生可能と判断された場合、コントローラ１１０６は、メモリカードインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ４、インタフェース１４２４、および端子１４２６を介してメモリカードインタフェース１２００へ出力する（ステップＳ７４２）。

【０３２８】再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ３を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１６へ与える。

【０３２９】そして、復号処理部１５１６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１０から出力されたライセンス鍵Ｋｃによって復号してコンテンツデータＤｃを取得する（ステップＳ７４４）。

【０３３０】そして、復号されたコンテンツデータＤｃは音楽再生部１５１８へ出力され、音楽再生部１５１８は、コンテンツデータを再生し、ＤＡ変換器１５１９はディジタル信号をアナログ信号に変換して端子１５３０へ出力する。そして、音楽データは端子１５３０から外部出力装置を介してヘッドホーン１３０へ出力されて再生される（ステップＳ７４６）。これによって再生動作が終了する。

【０３３１】上記においては、メモリカード１１０に記録された暗号化コンテンツデータを再生端末１００によって再生する場合について説明したが、パーソナルコンピュータ５０に、図７に示すコンテンツ再生デバイス１５５０を内蔵することによってライセンス管理モジュール５１１およびライセンス管理デバイス５２０によって受信された暗号化コンテンツデータを再生することが可能である。

【０３３２】図３１を参照して、パーソナルコンピュータ５０のライセンス管理モジュール５１１またはライセンス管理デバイス５２０によって受信された暗号化コンテンツデータおよびライセンスの管理について説明する。パーソナルコンピュータ５０のＨＤＤ５３０は、コンテンツリストファイル１５０と、コンテンツファイル１５３１～１５３５と、ライセンス管理ファイル１５２１～１５２５とを含む。

【０３３３】コンテンツリストファイル１５０は、所有するコンテンツの一覧形式のデータファイルであり、個々のコンテンツに対する情報（楽曲名、アーティスト名など）と、コンテンツファイルとライセンス管理ファイルとを示す情報（ファイル名）などが含まれている。個々のコンテンツに対する情報は受信時に付加情報Ｄｃ－ｉｎｆから必要な情報を取得して自動的に、あるいは、ユーザの指示によって記載される。また、コンテンツファイルのみ、ライセンス管理ファイルのみの再生できないコンテンツについても一覧の中で管理することが可能である。

【０３３４】コンテンツファイル１５３１～１５３５は、ライセンス管理モジュール５１１またはライセンス

管理デバイス５２０によって受信された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを記録するファイルであり、コンテンツごとに設けられる。

【０３３５】また、ライセンス管理ファイル１５２１～１５２５は、それぞれ、コンテンツファイル１５３１～１５３５に対応して記録されており、ライセンス管理モジュール５１１またはライセンス管理デバイス５２０によって受信されたライセンスを管理するためのファイルである。これまでの説明でも明らかなように、ライセンスは通常参照することができないが、ライセンス鍵Ｋｃを除く他の情報は、ユーザが書き換えることさえできなければ著作権保護の点では問題ない。しかし、運用においてライセンス鍵Ｋｃと分離して管理することはセキュリティの低下につながるため好ましくない。そこで、ライセンス配信を受ける場合に平文にて参照できるトランザクションＩＤ、コンテンツＩＤや、ライセンス購入条件ＡＣから容易に判断できるアクセス制御情報ＡＣmおよび再生制御情報ＡＣｐにて制限されている事項の写しを平文にて記録する。さらに、ライセンス管理デバイス５２０にライセンスが記録された場合にはエントリ番号を、ライセンス管理モジュール５１１の管理下にあるライセンスについては暗号化レベル１拡張ライセンス（ライセンスとチックアウト情報）を記録する。暗号化レベル１拡張ライセンスは、ライセンス管理モジュール５１１による独自な暗号化が施されている。独自な暗号化とは、パーソナルコンピュータ５０のコントローラ（ＣＰＵ）が個別に持つ番号やパーソナルコンピュータの起動プログラムであるＢＩＯＳのバージョン番号等のパーソナルコンピュータ５０から得られるパーソナルコンピュータ５０を特定できる情報に関連付けて暗号化を行なうものである。したがって、生成された暗号化レベル１ライセンスは、パーソナルコンピュータ５０に独自なライセンスになり、複製されても他の装置では意味を持たない。ライセンス管理デバイス５２０のメモリ５２１５のライセンス領域５２５Ｂは、高いセキュリティレベル（レベル２）でライセンスを記録する耐タンパモジュールで構成された記録領域である。ライセンス（ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、アクセス制限情報ＡＣm、ライセンスＩＤ）を記録するためにＮ個のエントリを備えている。

【０３３６】図３１を参照して、ライセンス管理ファイル１５２１，１５２４は、それぞれ、エントリ番号０，１を含む。これは、ライセンス管理デバイス５２０によって受信され、ライセンス管理デバイス５２０のメモリ５２１５のライセンス領域５２１５Ｂにおいて管理されるライセンス（ライセンスＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣmおよび再生制御情報ＡＣm）の管理領域を指定する番号であり、レベル２ライセンスに係るファイルである。

【０３３７】また、コンテンツファイル１５３１に記録されたファイル名の暗号化コンテンツデータを携帯電話機１００または再生端末１０２に装着されたメモリカード１１０へ移動させるとき、コンテンツファイル１５３１～１５３５を検索してコンテンツファイル１５３１を抽出すれば、暗号化コンテンツデータを再生するライセンスがどこで管理されているかが解かる。コンテンツファイル１５３１に対応するライセンス管理ファイル１５２１に含まれるエントリ番号は「０」であるので、コンテンツファイル１５３１に記録されたファイル名の暗号化コンテンツデータを再生するライセンスは、ライセンス管理デバイス５２０のメモリ５２１５のライセンス領域５２１５Ｂのエントリ番号０によって指定された領域に記録されている。そうすると、ＨＤＤ５３０に記録されたコンテンツリストファイル１５０のライセンス管理ファイル１５２１からエントリ番号０を読出し、その読出したエントリ番号０をライセンス管理デバイス５２０に入力することによって、メモリ５２１５のライセンス領域５２１５Ｂからライセンスを容易に取出し、メモリカード１１０へ移動できる。そして、ライセンスを移動した後は、メモリ５２１５のライセンス領域５２１５Ｂにおいて指定されたエントリ番号内のライセンスは削除されるので（図２０のステップＳ３５４，Ｓ３６６参照）、それに対応してライセンス管理ファイル１５２３のように「ライセンス無」が記録される（図２１のステップＳ３８６参照）。

【０３３８】ライセンス管理ファイル１５２３は、「ライセンス無」を含む。これは、ライセンス管理デバイス５２０によって受信されたライセンスが、移動された結果である。対応するコンテンツファイル１５３３はＨＤＤ５３０に記録されたままになっている。メモリカードからライセンスを再びライセンス管理モジュール５２０へ移動、あるいは、配信サーバ１０から再び配信を受ける場合には、ライセンスについてのみ配信を受けることが可能である。

【０３３９】また、ライセンス管理モジュール５１１によって受信された暗号化コンテンツデータのライセンスは、ライセンス管理ファイル１５２２，１５２５によって管理される。ライセンス管理ファイル１５２２，１５２５は、ライセンス管理モジュール５１１によって受信した暗号化コンテンツデータを再生するためのライセンスを含む（図１７のステップＳ２７８参照）。これは、上述したように、ライセンス管理モジュール５１１は、ソフト的に暗号化コンテンツデータおよびライセンスを受信するので、ライセンスをライセンス管理デバイス５２０に書込むことによって管理するのではなく、ファイルとしてＨＤＤ５３０に記録することにしたものである。

【０３４０】そうすると、たとえば、コンテンツファイル１５３３に記録されたファイル名の暗号化コンテンツデータを再生端末１０２に装着されたメモリカード１１

０へチェックアウトさせるとき、コンテンツファイル１５３１～１５３５を検索してコンテンツファイル１５３３を抽出し、コンテンツファイル１５３３に対応するライセンス管理ファイル１５２３からチェックアウト情報、およびライセンス等を読出すことができる。

【０３４１】このように、本発明においては、ライセンス管理モジュール５１１によって受信した暗号化コンテンツデータおよびライセンスと、ライセンス管理デバイス５２０によって受信した暗号化コンテンツデータおよびライセンスとを同じフォーマットで管理する。つまり、異なるセキュリティレベル（レベル１、レベル２）で受信した暗号化コンテンツデータおよびライセンスを統一したフォーマットによって管理する。このようにすることによって、異なるセキュリティレベルで暗号化コンテンツデータおよびライセンスを受信した場合でも、各セキュリティレベルを低下させることなく、著作権を保護しながら暗号化コンテンツデータの再生を自由に行なうことができる。

【０３４２】図３２は、メモリカード１１０のメモリ１４１５におけるデータ領域１４１５Ｃとライセンス領域１４１５Ｃを示したものである。データ領域１４１５Ｃには、再生リストファイル１６０とコンテンツファイル１６１１～１６１ｎと、ライセンス管理ファイル１６２１～１６２ｎとが記録されている。コンテンツファイル１６１１～１６１ｎは、受信した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを１つのファイルとして記録する。また、ライセンス管理ファイル１６２１～１６２ｎは、それぞれ、コンテンツファイル１６１１～１６１ｎに対応して記録されている。

【０３４３】メモリカード１１０は、配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信したとき、パーソナルコンピュータ５０から暗号化コンテンツデータおよびライセンスを「移動セッション」または「チェックアウトセッション」によって受信したとき、暗号化コンテンツデータおよびライセンスをメモリ１４１５に記録する。つまり、メモリカード１１０は、セキュリティレベルに無関係に暗号化コンテンツデータおよびライセンスをハード的（高いセキュリティレベルを意味する）に管理する。

【０３４４】したがって、パーソナルコンピュータ５０のライセンス管理デバイス５２０によって受信され、かつ、移動セッションによってメモリカード１１０に送信されたセキュリティレベルの高い暗号化コンテンツデータのライセンスと、ライセンス管理モジュール５１０によって受信され、かつ、チェックアウトセッションによってメモリカード１１０に送信されたセキュリティレベルの低い暗号化コンテンツデータのライセンスとは、メモリ１４１５のライセンス領域１４１５Ｂのエントリ番号によって指定された領域に記録され、メモリ１４１５のデータ領域１４１５Ｃに記録された再生リストファイル１６０のライセンス管理ファイルを読出せば、エントリ番号を取得でき、その取得したエントリ番号によって対応するライセンスをライセンス領域１４１５Ｂから読出すことができる。

【０３４５】また、ライセンス管理ファイル１６２２は、点線で示されているが、実際には記録されていないことを示す。コンテンツファイル１６１２は存在しているがライセンスが無く再生できないことを表しているが、これは、たとえば、再生端末が他の携帯電話機から暗号化コンテンツデータだけを受信した場合に相当する。

【０３４６】また、コンテンツファイル１６１３は、点線で示されているが、これは、たとえば、再生端末が配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータだけを他の携帯電話機へ送信した場合に相当し、ライセンスはメモリ１４１５に存在するが暗号化コンテンツデータが存在しないことを意味する。

【０３４７】［リッピング］パーソナルコンピュータ５０のユーザは配信によって暗号化コンテンツデータとライセンスを取得する他に、所有する音楽ＣＤから、音楽データを取得して利用することが可能である。著作権者の権利保護の立場から音楽ＣＤのデジタル複製は自由に行なっても良いものではないが、個人が自己の使用目的のために、著作権保護機能を備えるツールを用いて複製し、音楽を楽しむことは許されている。そこで、ライセンス管理モジュール５１１は、音楽ＣＤから音楽データを取得して、ライセンス管理モジュール５１１にて管理可能な暗号化コンテンツデータとライセンスを生成するリッピング機能を実現するプログラムも含んでいる。

【０３４８】また、近年の音楽ＣＤには、音楽データ内に、ウォーターマークと呼ばれる電子透かしを挿入したものがある。このウォーターマークには、著作権者によって利用者における利用の範囲が利用規則として書込まれている。利用規則が書込まれている音楽データからのリッピングでは、著作権保護の点から必ずこの利用規則に従う必要がある。以後、利用規則として、複製条件〈複製禁止・複製可能世代・複製可〉、複製の有効期間、最大チェックアウト数、編集、再生速度、再生可能な地域のコード、複製に対する再生回数制限、利用可能時間が記載されているとする。また、ウォーターマークが検出されない場合、すなわち、利用規則が書込まれていない従来の音楽ＣＤもある。

【０３４９】また、リッピングは、音楽ＣＤから、直接、音楽データを取得する他に、アナログ信号として入力された音楽信号を、デジタル化して音楽データとして取得する場合もある。さらには、データ量を減らすために圧縮符号化された音楽データを入力とすることも可能である。また、さらに、本実施の形態による配信システム以外の、配信システムにて配信されたコンテンツデー

タを入力として取り込むことも可能である。

【０３５０】図３３および図３４を参照して、音楽データが記録された音楽ＣＤからのリッピングによる暗号化コンテンツデータおよびライセンスの取得について説明する。

【０３５１】図３３は、図６に示すパーソナルコンピュータ５０に含まれるＣＤ－ＲＯＭドライブ５４０がＣＤから読出した音楽データをリッピングするソフトウエアの機能を示す機能ブロック図である。音楽データをリッピングするソフトウエアは、ウォーターマーク検出手段５４００と、ウォーターマーク判定手段５４０１と、リマーク手段５４０２と、ライセンス発生手段５４０３と、音楽エンコーダ５４０４と、暗号手段５４０５とを備える。

【０３５２】ウォーターマーク検出手段５４００は、音楽ＣＤから取得した音楽データからウォーターマークを検出し、記載されている利用規則を抽出する。ウォーターマーク判定手段５４０１は、ウォーターマーク検出手段５４００の検出結果、すなわち、ウォーターマークが検出できたか否か、さらに検出できた場合には、ウォーターマークで記載されていた利用規則に基づいて、リッピングの可否を判定する。この場合、リッピング可の場合、ウォーターマークの利用規則が無い、または音楽ＣＤに記録された音楽データの複製および移動が許可された利用規則がウォーターマークによって記録されていたことを意味し、リッピング不可の場合、音楽ＣＤに記録された音楽データを複製および移動してはいけない利用規則がウォーターマークによって記録されていたことを意味する。

【０３５３】リマーク手段５４０２は、ウォーターマーク判定手段５４０１における判定結果がリッピング可能で、複製世代の指示がある場合、つまり、音楽データを複製・移動して良い場合、音楽データに含まれるウォーターマークを音楽データの複製条件を変更したウォーターマークに付け替える。ただし、アナログ信号を入力してリッピングする場合や符号化された音楽データを入力とする場合、および他の配信システムにて配信された音楽データを入力とする場合には、リッピング可能であれば利用規則の内容に関わらず、必ず、ウォーターマークを付け替える。この場合、複製世代の指示がある場合は、利用規則の内容を変更して、それ以外の場合には取得した利用規則をそのまま利用する。

【０３５４】ライセンス発生手段５４０３は、ウォーターマーク判定手段５４０１の判定結果に基づいてライセンスを発生させる。音楽エンコーダ５４０４は、リマーク手段５４０２によってウォーターマークがリマークされた音楽データを所定の方式に符号化する。暗号手段５４０５は、音楽エンコーダ５４０４からの音楽データをライセンス発生手段５４０３により発生されたライセンスに含まれるライセンス鍵Ｋｃによって暗号化する。

【０３５５】図３４を参照して、パーソナルコンピュータ５０のコントローラ５１０におけるリッピング動作について説明する。リッピング動作が開始されると、ウォーターマーク検出手段５４００は、音楽ＣＤから検出したデータに基づいてウォーターマークの利用規則を検出する（ステップＳ８００）。そして、ウォーターマーク判定手段５４０１は、ウォーターマーク検出手段５４００の検出結果とウォーターマークとして記録されていた利用規則に基づいて複製が可能か否かを判定する（ステップＳ８０２）。ウォーターマークが検出され、利用規則によって複製が許可され、かつ、利用規則の内容がライセンス内のアクセス制御情報や再生制御情報にて対応可能な場合、リッピング可と判断され、ステップＳ８０４へ移行する。また、ウォーターマークが検出され、利用規則によって複製の禁止、または、ライセンス内のアクセス制御情報や再生制御情報にて対応不可の利用規則が記載されている場合、リッピング禁止と判断され、ステップＳ８２８へ移行してリッピング動作は終了する。装着されたＣＤにウォーターマークが含まれていない場合、ステップＳ８１０へ移行する。

【０３５６】ステップＳ８０２において、リッピング可と判断した場合、音楽ＣＤから音楽データが取込まれ、リマーク手段５４０２によって音楽データに含まれるウォーターマークが複製条件を変更したウォーターマークに付け替えられる（ステップＳ８０６）。すなわち、ウォーターマークの利用規則が３世代までの複製を許可している場合、複製世代を２回にしたウォーターマークに付け替える。そして、ライセンス発生手段５４０３は、利用規則を反映したライセンスを生成する。すなわち、ライセンス発生手段５４０３は、複製回数が２世代であるライセンスを生成する（ステップＳ８０６）。その後、ライセンス発生手段５４０３は、利用規則を反映したチェックアウト可能数を含むチェックアウト情報を生成する（ステップＳ８０８）。チェックアウト可能数については、記載がない場合、「３」とする。

【０３５７】一方、ステップＳ８０２において、ウォーターマークが検出されない場合、ライセンス発生手段５４０３は、ライセンスの複製および移動を禁止したライセンスを生成する（ステップＳ８１０）。その後、ライセンス発生手段５４０３は、初期値が３であるチェックアウト可能数を含むチェックアウト情報を生成する（ステップＳ８１２）。

【０３５８】ステップＳ８０８またはＳ８１２の後、音楽エンコーダ５４０４は、ウォーターマークがリマークされた音楽データを所定の方式に符合化してコンテンツデータ｛Ｄｃ｝を生成する（ステップＳ８１４）。そして、暗号手段５４０５は、音楽エンコーダ５４０４からの音楽データをライセンス発生手段５４０３により発生されたライセンスに含まれるライセンス鍵Ｋｃによって暗号化を行ない、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ

を生成する（ステップＳ８１６）。その後、音楽ＣＤに含まれる情報またはパーソナルコンピュータ５０のキーボード５６０から入力されたユーザ入力等によってコンテンツデータ｛Ｄｃ｝の付加情報Ｄｃ－ｉｎｆが生成される（ステップＳ８１８）。

【０３５９】そうすると、パーソナルコンピュータ５０のコントローラ５１０は、バスＢＳ２を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得し、ＨＤＤ５３０に記録する（ステップＳ８２２）。そして、コントローラ５１０は、生成されたライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生制御情報ＡＣｐ）とチェックアウト情報とに独自の暗号化を施した暗号化拡張ライセンスを生成する（ステップＳ８２２）。その後、コントローラ５１０は、暗号化拡張ライセンスと、平文のトランザクションＩＤおよびコンテンツＩＤを含み、かつ、ＨＤＤに記録した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、ＨＤＤ５３０に記録する（ステップＳ８２４）。最後に、コントローラ５１０は、ＨＤＤ５３０に記録されているコンテンツリストファイルに受理したコンテンツのファイル名を追記して（ステップＳ８２６）、リッピング動作が終了する（ステップＳ８２８）。

【０３６０】このように音楽ＣＤからリッピングによっても暗号化コンテンツデータとライセンスとを取得でき、取得されたライセンスは、配信サーバ１０から配信されたコンテンツとともに保護されて管理される。

【０３６１】図３５～３７を参照して、図３４に示すフローチャートのステップＳ８０６におけるライセンスの生成について詳細に説明する。ライセンス発生手段５４０３は、ライセンスとしてコンテンツＩＤ、トランザクションＩＤ、ライセンス鍵、アクセス制限情報（メモリカード１１０でのライセンス鍵の出力に対する制限）、再生制御情報（コンテンツ再生デバイス１５５０での再生条件）およびチェックアウト可能数を発生する。

【０３６２】図３５を参照して、コンテンツＩＤ１は、固定領域２と管理領域３とから成る。コンテンツＩＤは、１６ｂｙｔｅｓから成り、そのうち、１ｂｙｔｅが固定領域２に割り当てられ、１５ｂｙｔｅｓが管理領域３に割り当てられる。そして、固定領域２は、コンテンツＩＤ１がどこで生成されたかを示すものであり、コンテンツＩＤが配信サーバ１０で生成された場合とパーソナルコンピュータ５０で生成された場合とでは、異なる値が書込まれる。パーソナルコンピュータ５０においてコンテンツＩＤが生成された場合、つまり、ローカルにコンテンツＩＤが生成された場合、固定領域２には１６進で「００」が書込まれ、パーソナルコンピュータ５０以外でコンテンツＩＤが生成された場合、それ以外の値が固定領域２に書込まれる。

【０３６３】管理領域３は、各コンテンツデータを識別するための識別番号が書込まれ、複数のコンテンツデータに対して１つの識別番号が重複して付されることがないように管理される。

【０３６４】図３６を参照して、トランザクションＩＤ４は、固定領域５と管理領域６とから成る。トランザクションＩＤは、１２ｂｙｔｅｓから成り、そのうち、１ｂｙｔｅが固定領域５に割り当てられ、１１ｂｙｔｅｓが管理領域６に割り当てられる。そして、固定領域５は、固定フラグ７とリザーブ領域８とから成る。固定フラグ７には１ｂｉｔが割り当てられ、リザーブ領域８には７ｂｉｔｓが割り当てられる。固定フラグ７は、トランザクションＩＤ４がどんな目的で生成されたかを示すものであり、トランザクションＩＤが、配信の管理のために配信サーバ１０で生成された場合とローカル使用のためにパーソナルコンピュータ５０で生成された場合とでは、異なる値が書込まれる。ローカル使用のためにトランザクションＩＤが生成された場合、つまり、パーソナルコンピュータ５０で、リッピング、またはチェックインのためにローカルにトランザクションＩＤが生成された場合、固定領域６の固定フラグ７に「０」が書込まれ、配信目的でトランザクションＩＤが生成された場合、固定領域６の固定フラグ７に「１」が書込まれる。トランザクションＩＤは、乱数の発生によって生成される。

【０３６５】ライセンス鍵は、ライセンス発生時に２ｋｅｙによるＴｒｉｐｌｅ－ＤＥＳ方式における共通鍵であり、コンテンツデータの暗号化および復号に用い、乱数の発生によって発生される。

【０３６６】図３７を参照して、アクセス制御情報ＡＣｍは、再生可能回数Ｐｌａｙ＿ｃｏｕｎｔと、移動・複製制御情報Ｍｏｖｅ＿ｃｏｕｎｔとから成る。再生可能回数Ｐｌａｙ＿ｃｏｕｎｔ、移動・複製制御情報Ｍｏｖｅ＿ｃｏｕｎｔ、および保護レベルＳａｆｅ＿Ｌｅｖｅｌには、それぞれ、１ｂｙｔｅが割り当てられる。

【０３６７】再生可能回数Ｐｌａｙ＿ｃｏｕｎｔには、暗号化コンテンツデータの再生不可を示す「０」、暗号化コンテンツデータの再生可能回数を示す「１～２５４」、および暗号化コンテンツデータを無制限に再生できることを示す「２５５」のいずれかが書き込まれる。再生可能回数「１～２５４」が書き込まれたとき、暗号化コンテンツデータが再生される毎に再生可能回数は１づつ減じられる。

【０３６８】移動・複製制御情報Ｍｏｖｅ＿ｃｏｕｎｔには、暗号化コンテンツデータおよびライセンスの移動および複製が禁止されることを示す「０」、暗号化コンテンツデータおよびライセンスの移動が不可であり、かつ、暗号化コンテンツデータおよびライセンスの複製が制限付きで許可されることを示す「１～１５」、暗号化コンテンツデータおよびライセンスの移動が制限付きで

許可され、かつ、暗号化コンテンツデータおよびライセンスの複製が不可であることを示す「２４０～２５３」、暗号化コンテンツデータおよびライセンスの移動が許可され、かつ、暗号化コンテンツデータおよびライセンスの複製が禁止されることを示す「２５４」および暗号化コンテンツデータとライセンスとの移動および複製が無制限に許可されることを示す「２５５」のいずれかが書き込まれる。移動・複製制御情報Ｍｏｖｅ＿ｃｏｕｎｔに「１～１５」が書き込まれたとき、暗号化コンテンツデータおよびライセンスが複製される毎に数値が１づつ減じられる。そして、数値が「０」になったとき、暗号化コンテンツデータおよびライセンスの移動および複製が禁止される。また、移動・複製制御情報Ｍｏｖｅ＿ｃｏｕｎｔに「２４０～２５３」が書き込まれたとき、暗号化コンテンツデータおよびライセンスが移動される毎に数値が１づつ増加される。そして、数値が２５４に達したとき、暗号化コンテンツデータおよびライセンスの移動が許可され、暗号化コンテンツデータおよびライセンスの複製が禁止される。なお、「１７～２３９」は未使用である。

【０３６９】保護レベルＳａｆｅ＿Ｌｅｖｅｌは、ライセンスに必要とするセキュリティレベルを数値化したものである。将来的に、暗号処理に使う鍵の長さ、ライセンスを記録するセキュリティ強度などを変更した場合などに対応できるように配置した。例えば、上述したライセンス管理モジュールのようにプログラムを用いてソフトウエアによってセキュリティを確保し、コンテンツを保護するより、メモカード１１０やコンテンツ再生デバイス１５５０のように、ハードウエアによってセキュリティを確保し、コンテンツを保護するほうがセキュリティレベルが高いこととなる。

【０３７０】再生制御情報ＡＣｐは、１ｂｙｔｅのｆｌａｇと、ｆｌａｇによって手有効となる複数の情報とからなる。ｆｌａｇ（ｉ）とは、１ｂｙｔｅのｆｌａｇのｉビット目を示す。そして、再生制御情報ＡＣｐは、ｆｌａｇ（０）、ｆｌａｇ（１）、ｆｌａｇ（２）＋Ｐｌａｙ＿ｌｅｎｇｔｈ、ｆｌａｇ（３）＋ｎｏｔ＿ａｆｔｅｒ、ｆｌａｇ（４）ｎｏｔ＿ｂｅｆｏｒｅ、ｆｌａｇ（５）＋Ｒｅｇｉｏｎ＿ｃｏｄｅから成る。

【０３７１】ｆｌａｇ（０）は、暗号化コンテンツデータの再生速度の変換の可否を示する。ｆｌａｇ（１）は、暗号化コンテンツデータの編集の可否を示す。ｆｌａｇ（２）＋Ｐｌａｙ＿ｌｅｎｇｔｈは、暗号化コンテンツデータの再生可能なサイズを示し、部分再生するときは、その部分再生のサイズを示す。ｆｌａｇ（３）＋ｎｏｔ＿ａｆｔｅｒは、暗号化コンテンツデータの利用が終了する日時を示す。ｆｌａｇ（４）ｎｏｔ＿ｂｅｆｏｒｅは、暗号化コンテンツデータの利用を開始できる日時を示す。ｆｌａｇ（５）＋Ｒｅｇｉｏｎ＿ｃｏｄｅは、暗号化コンテンツデータの地域コードを示す。なお、ｆｌａｇ（３）＋ｎｏｔ＿ａｆｔｅｒおよびｆｌａｇ（４）ｎｏｔ＿ｂｅｆｏｒｅにおける暗号化コンテンツデータの利用とは、暗号化コンテンツデータの再生、移動、複製、チェックアウト、およびチェックインを意味する。

【０３７２】チェックアウト可能数ｃｈｅｃｋｏｕｔ＿ｃｏｕｎｔには、チェックアウトを禁止する「０」と、チェックアウト可能な回数を示す「１以上の数」とのいずれかが書き込まれる。そして、チェックアウト可能数ｃｈｅｃｋｏｕｔ＿ｃｏｕｎｔに「１以上の数」が書き込まれたとき、チェックアウトされる毎に数値が１づつ減じられ、チェックインされる毎に数値が１づつ増加される。

【０３７３】ライセンス発生手段５４０３は、上述した内容のコンテンツＩＤ、トランザクションＩＤ、ライセンス鍵、アクセス制限情報ＡＣｍおよび再生制御情報ＡＣｐからライセンスと、チェックアウト可能数ｃｈｅｃｋｏｕｔ＿ｃｏｕｎｔとをリッピング時に発生する。

【０３７４】なお、音楽ＣＤからリッピングによって取得された暗号化コンテンツデータおよびライセンスは、ライセンス管理モジュール５１１によって受信された暗号化コンテンツデータおよびライセンスと同じようにソフトウエアによって管理される。

【０３７５】上記においては、パーソナルコンピュータ５０は、音楽ＣＤからリッピングによって暗号化コンテンツデータおよびライセンスを取得したが、本発明においては、これに限らず、インターネット配信によって受信したコンテンツデータからリッピングによって暗号化コンテンツデータおよびライセンスを生成しても良い。パーソナルコンピュータ５０は、図１および図２に示すインターネット網３０を用いて配信サーバ１０との間で公開鍵および共通鍵等をやり取りし、相互認証を行ないながら暗号化コンテンツデータおよびライセンスを受信するが、リッピングにより暗号化コンテンツデータおよびライセンスを取得するときは、このような公開鍵および共通鍵のやり取りを行なわずに、コンテンツデータを通常のインターネット配信によって受信する。

【０３７６】したがって、パーソナルコンピュータ５０は、通常のインターネットに接続されていないときは、音楽ＣＤからリッピングによって暗号化コンテンツデータおよびライセンスを取得でき、通常のインターネットに接続されているときは、そのインターネットによって配信されるコンテンツデータからリッピングによって暗号化コンテンツデータおよびライセンスを取得できる。そのため、本発明において、パーソナルコンピュータ５０が暗号化コンテンツデータおよびライセンスを取得するためには、必ずしもインターネットに接続されている必要はなく、ＣＤ－ＲＯＭドライブを内蔵していれば良い。そして、リッピングによって暗号化コンテンツデータおよびライセンスを取得する場合、パーソナルコンピ

ュータは、ライセンス管理デバイス５２０やライセンス管理モジュール５１１を内蔵している必要はなく、図３３に示した機能ブロック図の各手段によって実行されるソフトウエアを内蔵していれば良い。

【０３７７】もちろん、本発明によるパーソナルコンピュータは、リッピングによって暗号化コンテンツデータおよびライセンスを取得する機能の他に、ライセンス管理デバイス５２０やライセンス管理モジュール５１１によって暗号化コンテンツデータおよびライセンスを受信する機能をもっていても良い。

【０３７８】なお、リッピングによるライセンスは、パーソナルコンピュータ５０によって生成されるため、そのライセンスを「ローカルライセンス」と言う。

【０３７９】本発明の実施の形態によれば、パーソナルコンピュータは、音楽ＣＤからまたはインターネット配信によってコンテンツデータを取得し、そのコンテンツデータに含まれるウォーターマーク（複製可否情報とも言う。）の内容に応じて暗号化コンテンツデータおよびライセンスを生成するので、リッピングによってウォーターマークの内容に応じた暗号化コンテンツデータおよびローカルライセンスの生成が可能である。

【０３８０】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　他のデータ配信システムを概念的に説明する概略図である。

【図３】　図１および図２に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１および図２に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図５】　図１および図２に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図６】　図１および図２に示すデータ配信システムにおけるパーソナルコンピュータの構成を示す概略ブロック図である。

【図７】　図２に示すデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

【図８】　図１および図２に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図９】　図６に示すパーソナルコンピュータに内蔵されたライセンス管理デバイスの構成を示す概略ブロック図である。

【図１０】　図１および図２に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第１のフローチャートである。

【図１１】　図１および図２に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第２のフローチャートである。

【図１２】　図１および図２に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第３のフローチャートである。

【図１３】　図１および図２に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第４のフローチャートである。

【図１４】　図１および図２に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第１のフローチャートである。

【図１５】　図１および図２に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第２のフローチャートである。

【図１６】　図１および図２に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第３のフローチャートである。

【図１７】　図１および図２に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第４のフローチャートである。

【図１８】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第１のフローチャートである。

【図１９】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第２のフローチャートである。

【図２０】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第３のフローチャートである。

【図２１】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第４のフローチャートである。

【図２２】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第１のフローチャートである。

【図２３】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第２のフローチャートである。

【図２４】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第３のフローチャートである。

【図２５】　図１および図２に示すデータ配信システム

における暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第４のフローチャートである。

【図２６】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックイン動作を説明するための第１のフローチャートである。

【図２７】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックイン動作を説明するための第２のフローチャートである。

【図２８】　図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックイン動作を説明するための第３のフローチャートである。

【図２９】　携帯電話機における再生動作を説明するための第１のフローチャートである。

【図３０】　携帯電話機における再生動作を説明するための第２のフローチャートである。

【図３１】　パーソナルコンピュータのハードディスクにおけるコンテンツリストファイルの構成を示す図である。

【図３２】　メモリカードにおける再生リストファイルの構成を示す図である。

【図３３】　リッピングを実行するソフトウエアの機能を説明するための機能ブロック図である。

【図３４】　図１および図２に示すデータ配信システムにおけるリッピングの動作を説明するためのフローチャートである。

【図３５】　コンテンツＩＤのフォーマット図である。

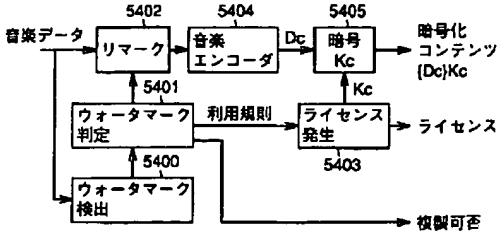
【図３６】　トランザクションＩＤのフォーマット図である。

【図３７】　メディアアクセス条件、デコーダアクセス条件およびチェックアウト可能数の構成を説明すための図表である。

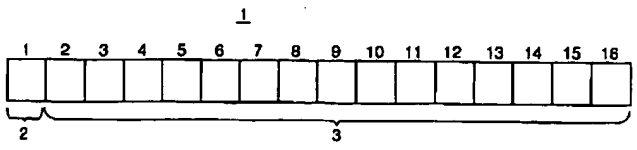
【符号の説明】

１　コンテンツＩＤ、２，５　固定領域、３，６　管理領域、４　トランザクションＩＤ、７　ＭＳＢ　８　リザーブ、１０　配信サーバ、２０　配信キャリア、３０　インターネット網、４０　モデム、５０　パーソナルコンピュータ、６０　ＣＤ、７０　ＵＳＢケーブル、１００，１０２　携帯電話機、１１０　メモリカード、１３０　ヘッドホーン、１５０　コンテンツリストファイル、１６０　再生リストファイル、３０２　課金データベース、３０４　情報データベース、３０６　ＣＲＬデータベース、３０７　メニューデータベース、３０８　配信記録データベース、３１０　データ処理部、３１２，３２０，１４０４，１４０８，１４１２，１４２２，１５０４，１５１０，１５１６，５２０４，５２０８，５２１２，５２２２　復号処理部、３１３　認証鍵保持部、３１５　配信制御部、３１６，　セッションキー発生部、３１８，３２６，３２８，１４０６，１４１０，１４１７，１５０６，５２０６，５２１０，５２１７，５４０５　暗号処理部、３５０　通信装置、５１０，１１０６，１４２０，５２２０　コントローラ、５１１　ライセンス管理モジュール、５２０　ライセンス管理デバイス、５３０　ハードディスク、５４０　ＣＤ－ＲＯＭドライブ、５５０，１１１２ＵＳＢインタフェース、５６０　キーボード、５７０　ディスプレイ、５８０，１１１４，１４２６，１５３０，５２２６　端子、１１０８　操作パネル、１１１０　表示パネル、１２００　メモリカードインタフェース、１４００，１５００，５２００　認証データ保持部、１４０２，５２０２　Ｋｍｃ保持部、１４１４，５２１４　ＫＰａ保持部、１４１５，５２１５　メモリ、１４１５Ａ，５２１５Ａ　ＣＲＬ領域、１４１５Ｂ　再生リスト、１４１５Ｃ，５２１５Ｂ　ライセンス領域、１４１５Ｄ　データ領域、１４１６，５２１６　ＫＰｍｃ保持部、１４１８，５２１８　セッションキー発生部、１４２１，５２２１　Ｋｍ保持部、１４２４，５２２４　インタフェース、１４４２，１４４６　切換スイッチ、１５０２　Ｋｐ１保持部、１５１８　音楽再生部、１５１９　ＤＡ変換器、１５２１～１５２５，１６２１～１６２ｎ　ライセンス管理ファイル、１５３１～１５３５，１６１１～１６１ｎ　コンテンツファイル、１５５０　コンテンツ再生デバイス、５４００　ウォーターマーク検出手段、５４０１　ウォーターマーク判定手段、５４０２　リマーク手段、５４０３　ライセンス発生手段、５４０４　音楽エンコーダ。

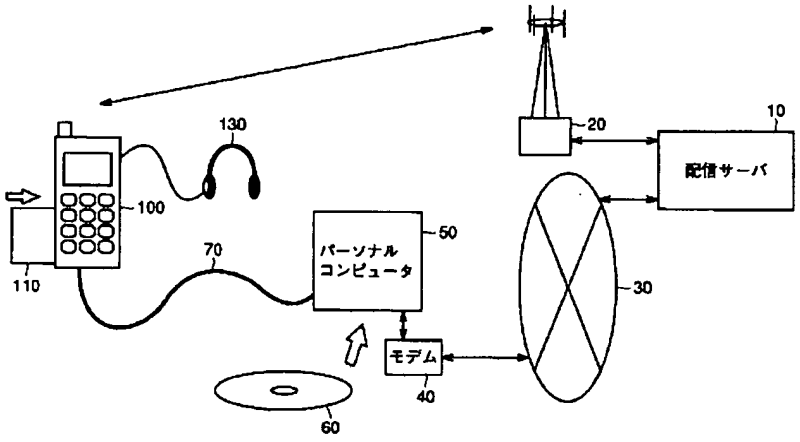
【図３３】



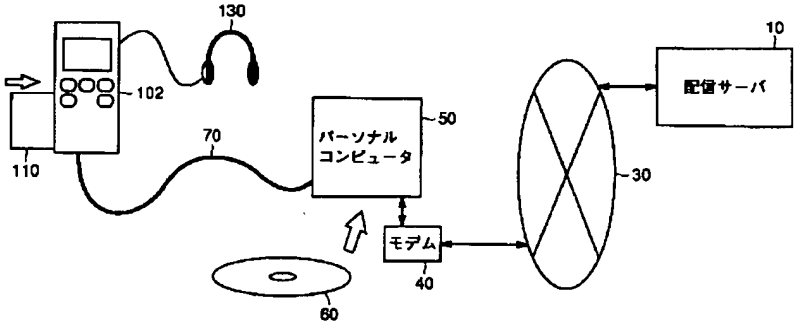
【図３５】



【図１】



【図２】



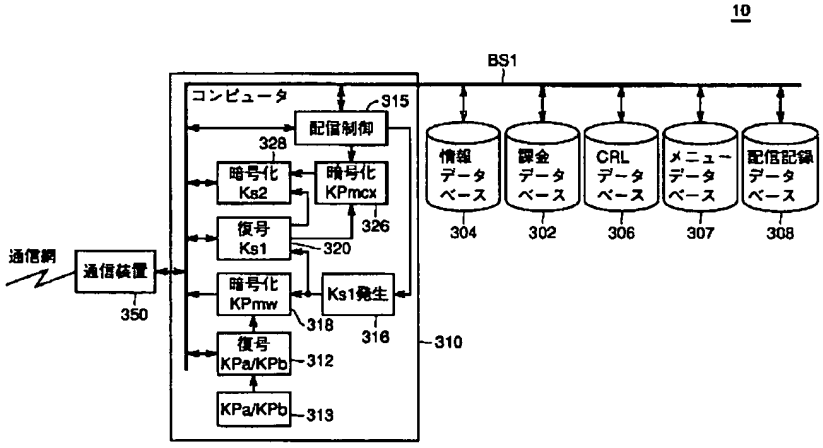
【図３】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ {Dc}Kcとして配信され、メモリカードに保持される
Dc-inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
トランザクションID	ライセンス	ライセンス固有	配信を特定するための管理コード
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	トランザクションID＋コンテンツIDの総称
ライセンス	ライセンス	ライセンス固有	Kc＋ACm＋ACp＋ライセンスIDの総称
CRL	禁止クラスリスト	システム共通	使用禁止認証データのリスト CRLの更新日(CRLdate)を含む

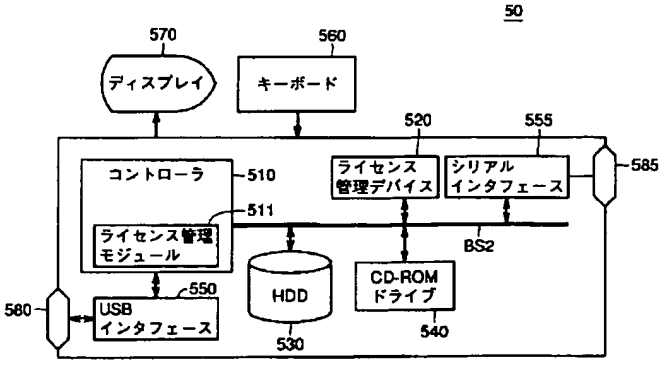
【図４】

	記号	種類	属性	特性
配信サーバ	KPa/KPb	公開認証鍵	システム共通	認証局にて認証データを復号する鍵 KPaはレベル1、KPbはレベル2
	Ks1	共通鍵	セッション固有	メモリカード、ライセンス管理デバイス、ライセンス管理モジュールへのライセンス配信ごとに発生
メモリカード ライセンス管理デバイス（ハードタンパ）	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵 配信サーバのKPaと同一
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵
ライセンス管理モジュール（ソフトタンパ）	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間のライセンスの授受ごとに発生
	Cmw	証明書	クラス証明書	メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書。認証機能を有する。 (KPmw//Cmw)KPa又は(KPmw//Cmw)KPbの形式で出荷時に記録。 ＊メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラスwごとに異なる。
コンテンツ再生デバイス	KPpy	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間の再生セッションごとに発生
	Cpy	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 (KPpy//Cpy)KPaの形式で出荷時に記録。 ＊コンテンツ再生デバイスのクラスyごとに異なる。

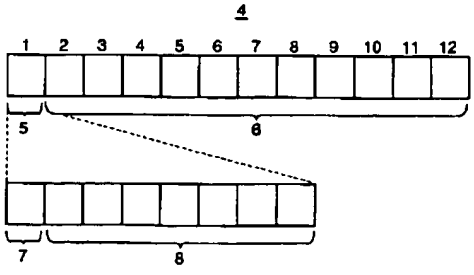
【図５】



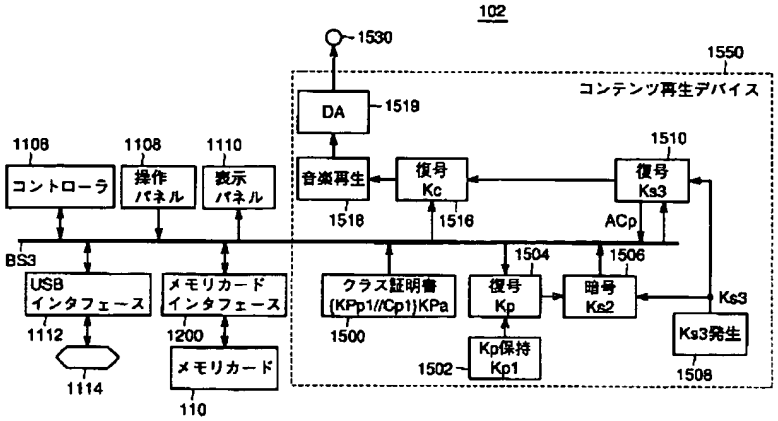
【図６】



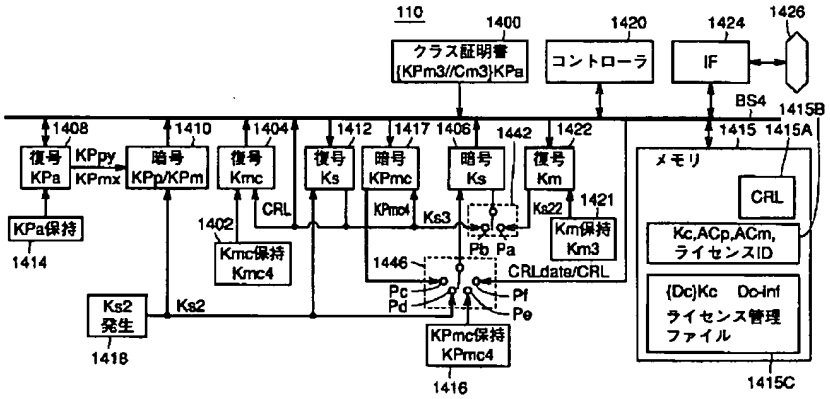
【図３６】



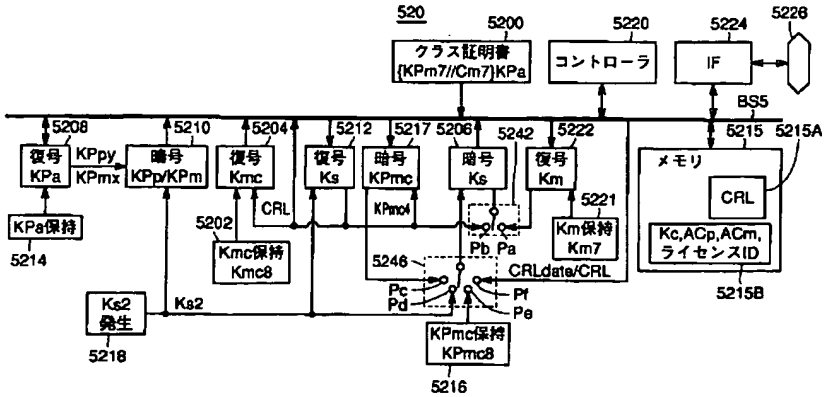
【図７】


102
1530
1550
コンテンツ再生デバイス
DA
1519
1108
1108
1110
1510
コントローラ
操作パネル
表示パネル
音楽再生
復号 Kc
復号 Ks3
1518
1516
ACp
BS3
1504
1506
USB インタフェース
メモリカード インタフェース
クラス証明書 {KPp1//Cp1}KPa
復号 Kp
暗号 Ks2
Ks3
1112
1200
1500
Kp保持 Kp1
Ks3発生
1502
1508
1114
メモリカード
110

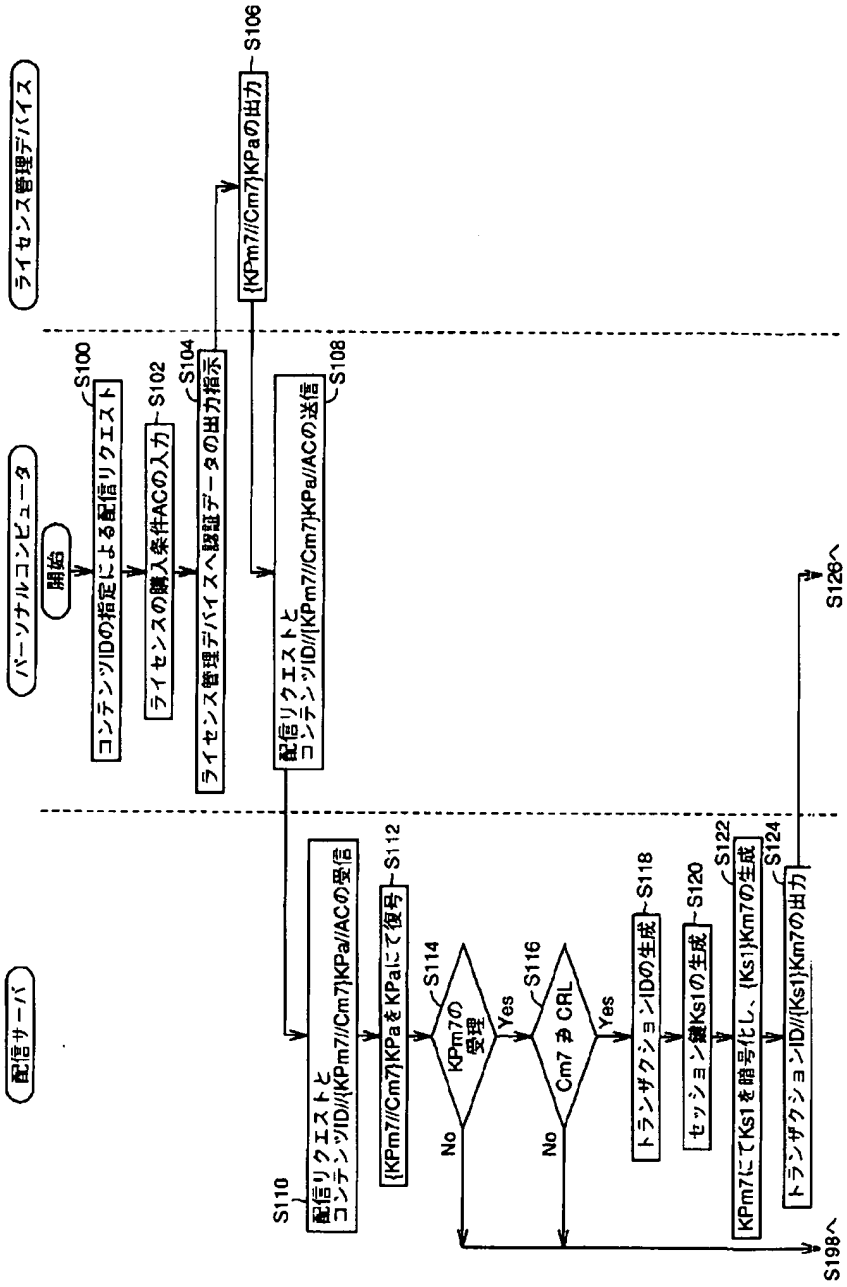
【図８】


110
1400
1420
1424
1426
クラス証明書 {KPm3//Cm3}KPa
コントローラ
IF
BS4
1415B
1408
1410
1404
1412
1417
1406
1442
1422
1415
1415A
復号 KPa
KPpy KPmx
暗号 KPp/KPm
復号 Kmc
復号 Ks
暗号 KPmc
暗号 Ks
復号 Km
メモリ
CRL
KPa保持
1414
1402
CRL
KPmc4
Ks3
Ks22
1421
Km保持 Km3
Kmc保持 Kmc4
Kc,ACp,ACm, ライセンスID
1446
Pb Pa
CRLdate/CRL
Pc
Pd
Pf
Pe
{Dc}Kc Dc-inf ライセンス管理 ファイル
Ks2 発生
Ks2
1418
KPmc保持 KPmc4
1416
1415C

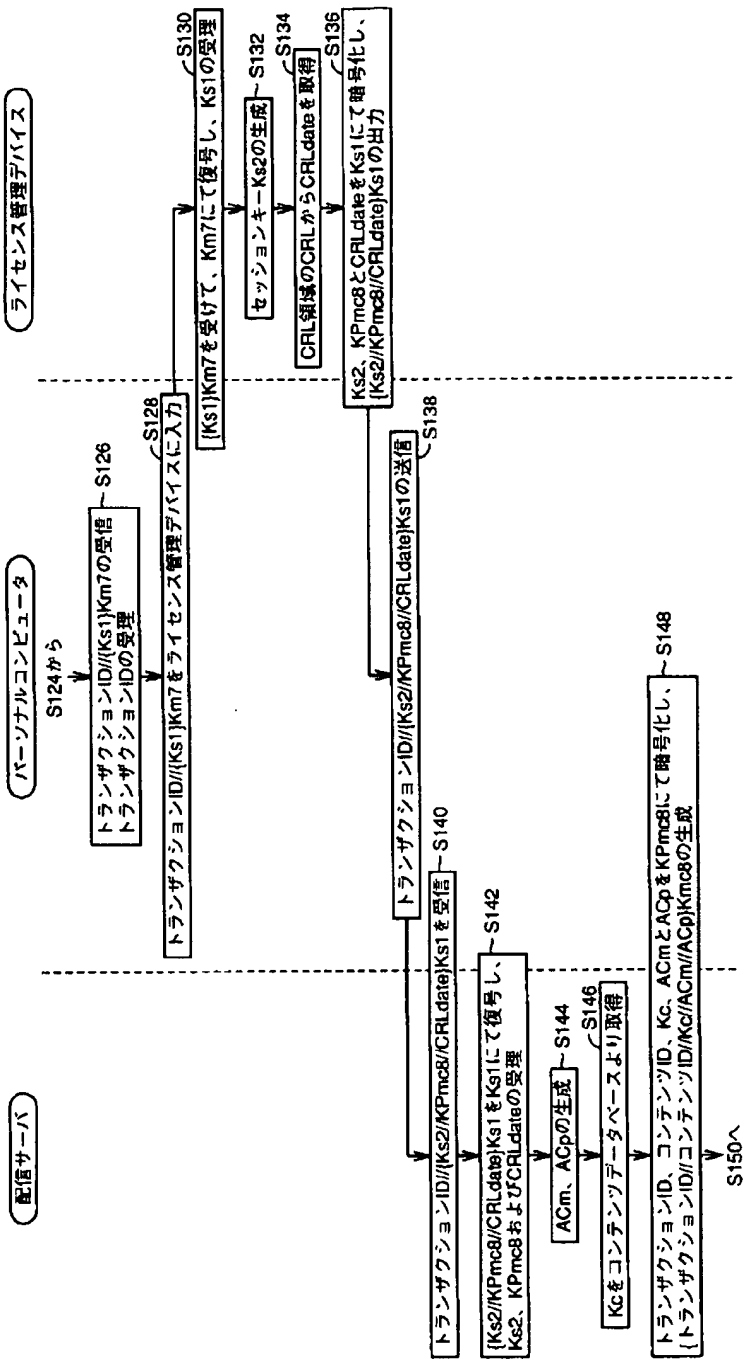
【図９】


520
5200
5220
5224
5226
クラス証明書 {KPm7//Cm7}KPa
コントローラ
IF
BS5
5208
5210
5204
5212
5217
5206
5242
5222
5215
5215A
復号 KPa
KPpy KPmx
暗号 KPp/KPm
復号 Kmc
復号 Ks
暗号 KPmc
暗号 Ks
復号 Km
メモリ
CRL
KPa保持
5214
5202
CRL
KPmc4
5221
Km保持 Km7
Kmc保持 Kmc8
Kc,ACp,ACm, ライセンスID
5246
Pb Pa
CRLdate/CRL
Pc
Pd
Pf
Pe
Ks2 発生
Ks2
5218
KPmc保持 KPmc8
5216
5215B

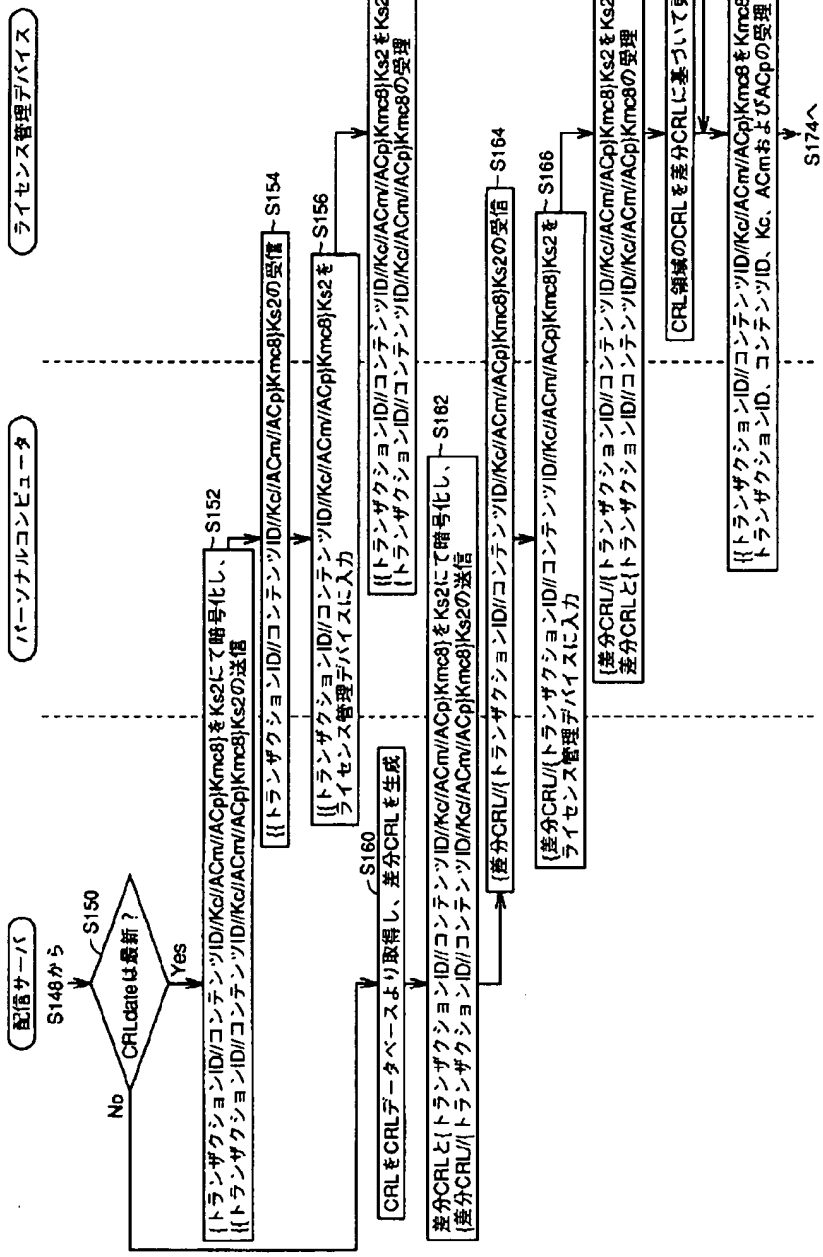
【図１０】


ライセンス管理デバイス
パーソナルコンピュータ
配信サーバ
開始
コンテンツIDの指定による配信リクエスト
S100
ライセンスの購入条件ACの入力
S102
ライセンス管理デバイスへ認証データの出力指示
S104
{KPm7//Cm7}KPaの出力
S106
配信リクエストとコンテンツID//{KPm7//Cm7}KPa//ACの送信
S108
配信リクエストとコンテンツID//{KPm7//Cm7}KPa//ACの受信
S110
{KPm7//Cm7}KPaをKPaにて復号
S112
KPm7の受理
S114
No
Yes
Cm7 ≠ CRL
S116
No
Yes
トランザクションIDの生成
S118
セッション鍵Ks1の生成
S120
KPm7にてKs1を暗号化し、{Ks1}Km7の生成
S122
トランザクションID//{Ks1}Km7の出力
S124
S198へ
S128へ

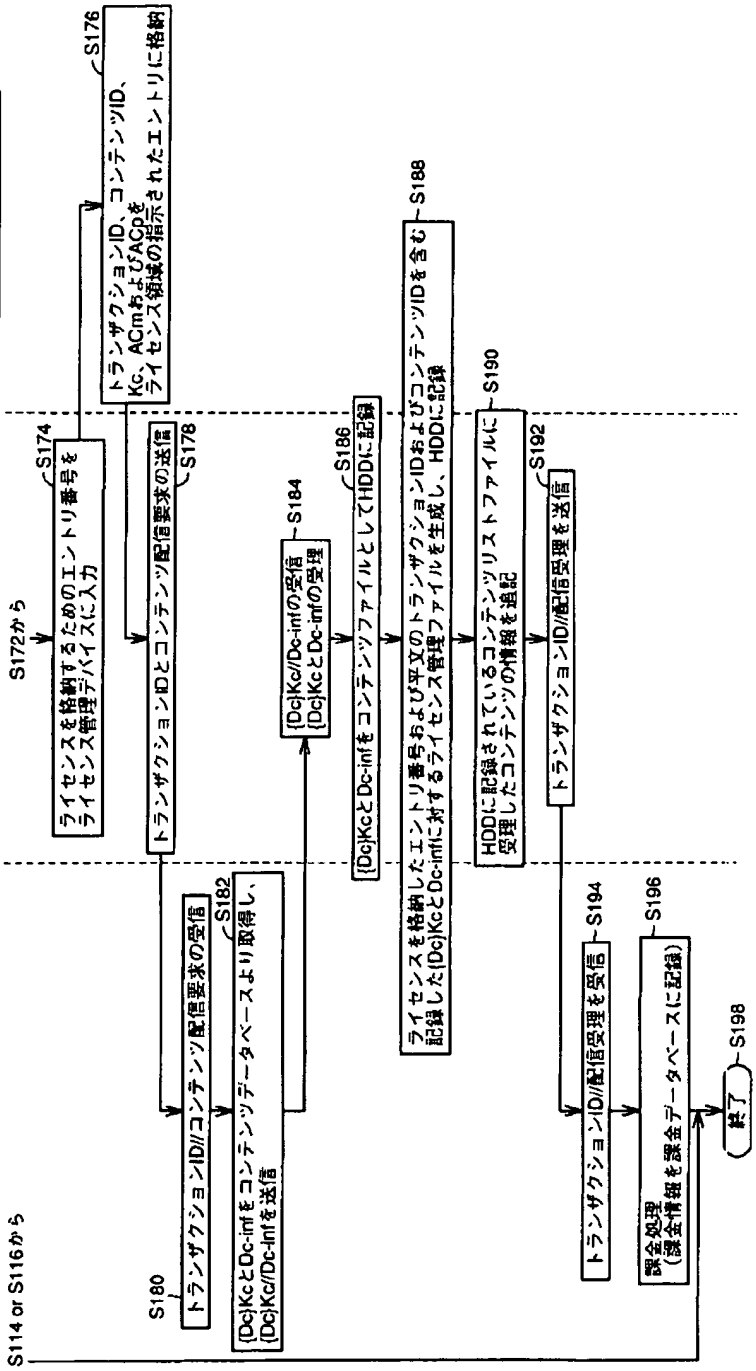
【図１１】


パーソナルコンピュータ
ライセンス管理デバイス
配信サーバ
S124から
トランザクションID//{Ks1}Km7の受信
トランザクションIDの受理
S126
トランザクションID//{Ks1}Km7をライセンス管理デバイスに入力
S128
{Ks1}Km7を受けて、Km7にて復号し、Ksiの受理
S130
セッションキーKs2の生成
S132
CRL領域のCRLからCRLdateを取得
S134
Ks2、KPmc8とCRLdateをKs1にて暗号化し、
{Ks2//KPmc8//CRLdate}Ks1の出力
S136
トランザクションID//{Ks2//KPmc8//CRLdate}Ksiの送信
S138
トランザクションID//{Ks2//KPmc8//CRLdate}Ks1を受信
S140
{Ks2//KPmc8//CRLdate}Ks1をKs1にて復号し、
Ks2、KPmc8およびCRLdateの受理
S142
ACm、ACpの生成
S144
Kcをコンテンツデータベースより取得
S146
トランザクションID、コンテンツID、Kc、ACmとACpをKPmc8にて暗号化し、
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8の生成
S148
S150へ

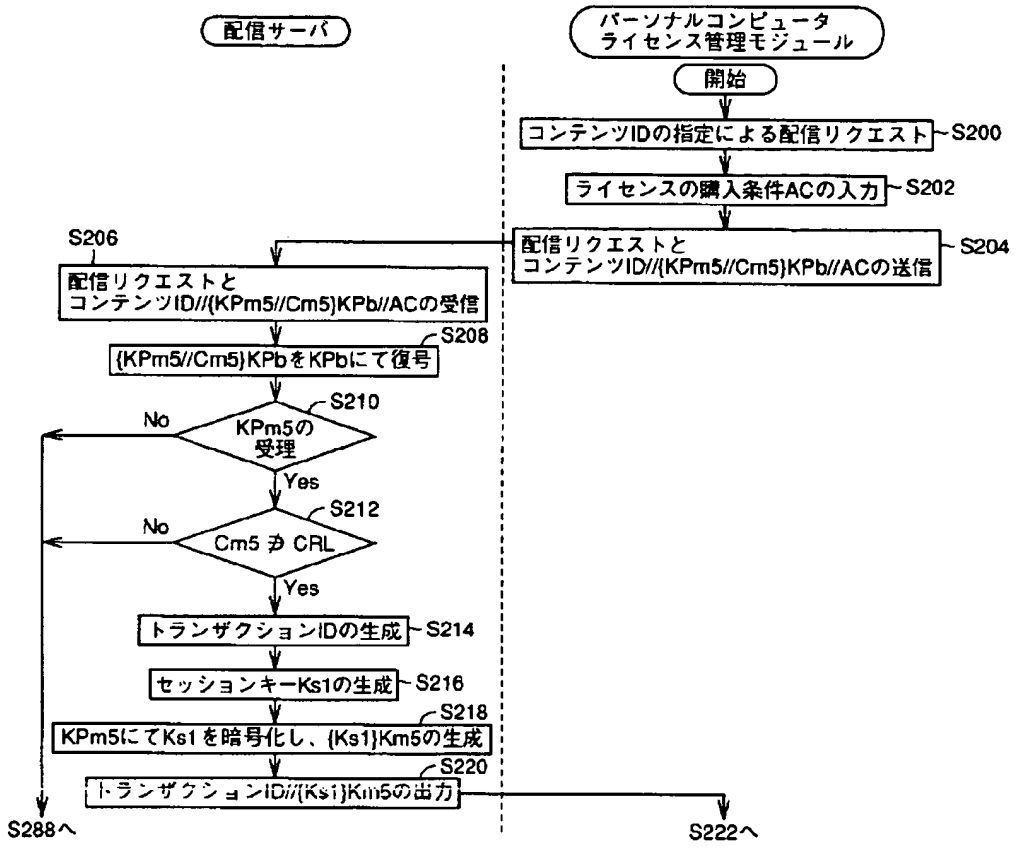
【図１２】


配信サーバ
パーソナルコンピュータ
ライセンス管理デバイス
S148から
S150
CRLdateは最新？
No
Yes
S152
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}をKs2にて暗号化し、
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2の送信
S154
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2の受信
S156
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を
ライセンス管理デバイスに入力
S158
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2をKs2にて復号
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8の受理
S160
CRLをCRLデータベースより取得し、差分CRLを生成
S162
差分CRLと{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}をKs2にて暗号化し、
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2の送信
S164
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2の受信
S166
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を
ライセンス管理デバイスに入力
S168
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2をKs2にて復号
差分CRLと{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8の受理
S170
CRL領域のCRLを差分CRLに基づいて更新する
S172
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8をKmc8にて復号
トランザクションID、コンテンツID、Kc、ACmおよびACpの受理
S174へ

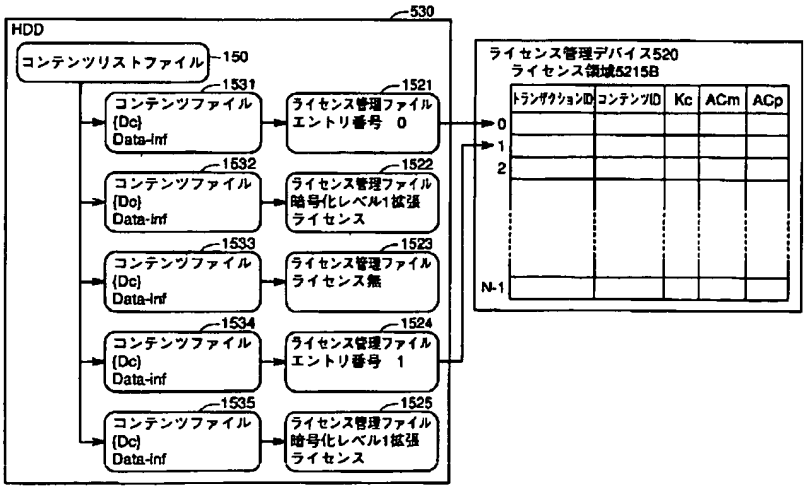
【図１３】


ライセンス管理デバイス
パーソナルコンピュータ
配信サーバ
S114 or S116から
S172から
ライセンスを格納するためのエントリ番号をライセンス管理デバイスに入力
S174
トランザクションID、コンテンツID、Kc、ACmおよびACpをライセンス領域の指示されたエントリに格納
S176
トランザクションIDとコンテンツ配信要求の送信
S178
トランザクションID//コンテンツ配信要求の受信
S180
S182
{Dc}KcとDc-infをコンテンツデータベースより取得し、{Dc}Kc//Dc-infを送信
{Dc}Kc//Dc-infの受信
{Dc}KcとDc-infの受理
S184
{Dc}KcとDc-infをコンテンツファイルとしてHDDに記録
S186
ライセンスを格納したエントリ番号および平文のトランザクションIDおよびコンテンツIDを含む記録した{Dc}KcとDc-infに対するライセンス管理ファイルを生成し、HDDに記録
S188
HDDに記録されているコンテンツリストファイルに受理したコンテンツの情報を追記
S190
トランザクションID//配信受理を送信
S192
トランザクションID//配信受理を受信
S194
課金処理（課金情報を課金データベースに記録）
S196
終了
S198

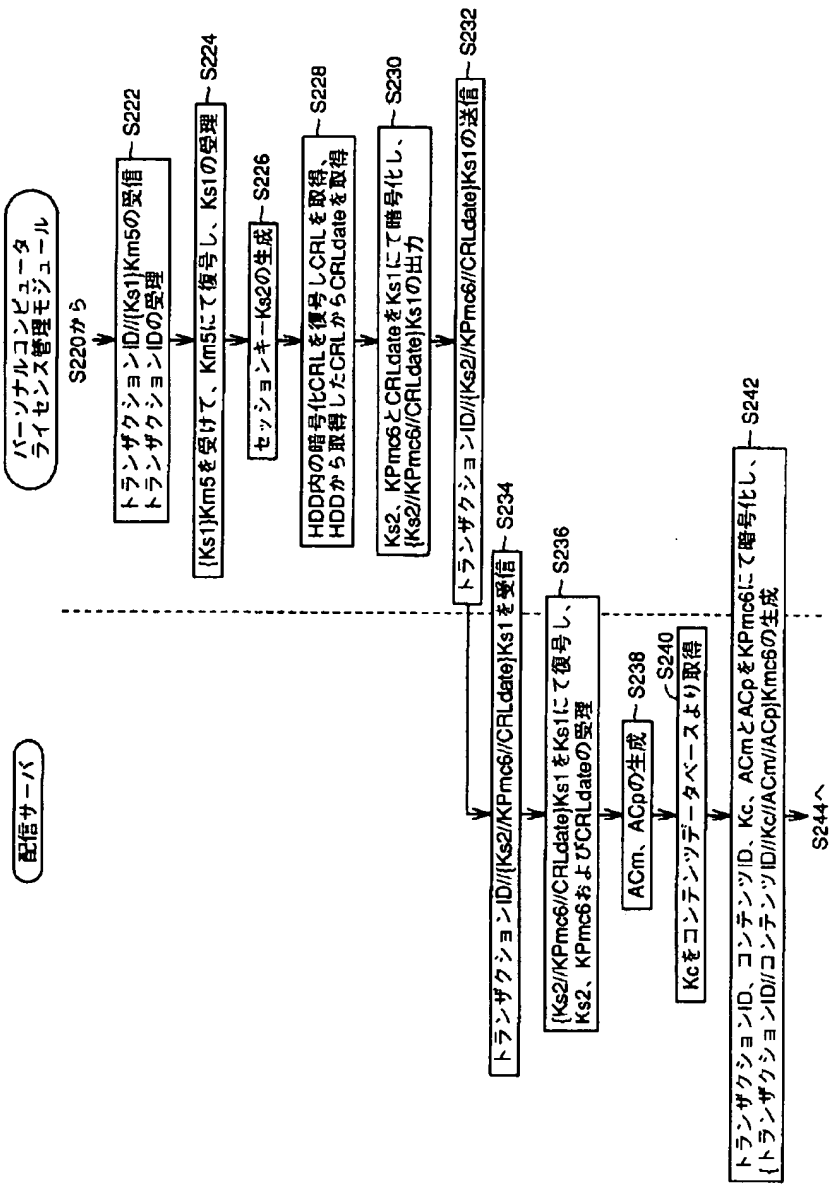
【図１４】


配信サーバ
パーソナルコンピュータ
ライセンス管理モジュール
開始
コンテンツIDの指定による配信リクエスト
S200
ライセンスの購入条件ACの入力
S202
配信リクエストと
コンテンツID//{KPm5//Cm5}KPb//ACの送信
S204
S206
配信リクエストと
コンテンツID//{KPm5//Cm5}KPb//ACの受信
S208
{KPm5//Cm5}KPbをKPbにて復号
S210
No
KPm5の
受理
Yes
S212
No
Cm5 ∌ CRL
Yes
トランザクションIDの生成
S214
セッションキーKs1の生成
S216
S218
KPm5にてKs1を暗号化し、{Ks1}Km5の生成
S220
トランザクションID//{Ks1}Km5の出力
S288へ
S222へ

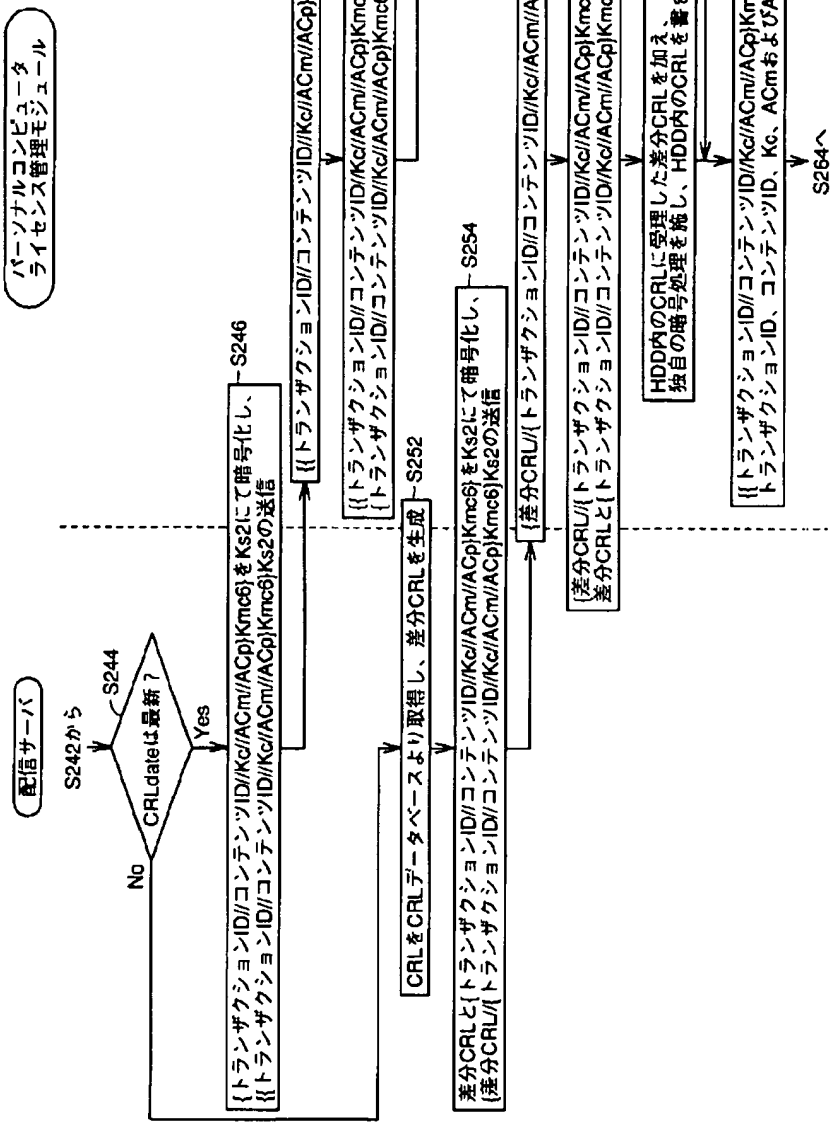
【図３１】


530
HDD
コンテンツリストファイル
150
1531
コンテンツファイル
{Dc}
Data-inf
1521
ライセンス管理ファイル
エントリ番号 0
1532
コンテンツファイル
{Dc}
Data-inf
1522
ライセンス管理ファイル
暗号化レベル1拡張
ライセンス
1533
コンテンツファイル
{Dc}
Data-inf
1523
ライセンス管理ファイル
ライセンス無
1534
コンテンツファイル
{Dc}
Data-inf
1524
ライセンス管理ファイル
エントリ番号 1
1535
コンテンツファイル
{Dc}
Data-inf
1525
ライセンス管理ファイル
暗号化レベル1拡張
ライセンス
ライセンス管理デバイス520
ライセンス領域5215B
トランザクションID
コンテンツID
Kc
ACm
ACp
0
1
2
N-1

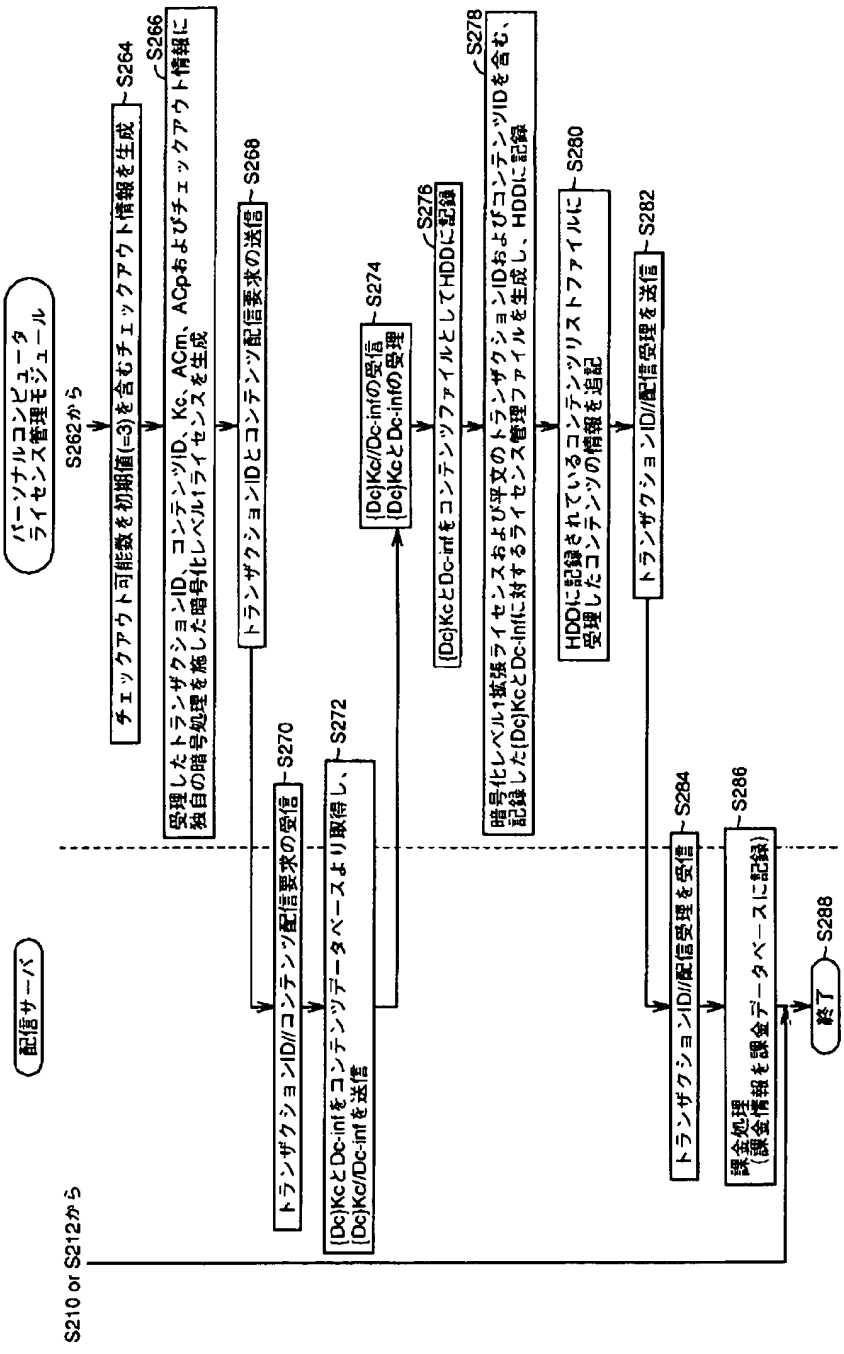
【図15】


パーソナルコンピュータ
ライセンス管理モジュール
S220から
トランザクションID//{Ks1}Km5の受信
トランザクションIDの受理
S222
{Ks1}Km5を受けて、Km5にて復号し、Ks1の受理
S224
セッションキーKs2の生成
S226
HDD内の暗号化CRLを復号しCRLを取得、
HDDから取得したCRLからCRLdateを取得
S228
Ks2、KPmc6とCRLdateをKs1にて暗号化し、
{Ks2//KPmc6//CRLdate}Ks1の出力
S230
トランザクションID//{Ks2//KPmc6//CRLdate}Ks1の送信
S232
配信サーバ
トランザクションID//{Ks2//KPmc6//CRLdate}Ks1を受信
S234
{Ks2//KPmc6//CRLdate}Ks1をKs1にて復号し、
Ks2、KPmc6およびCRLdateの受理
S236
ACm、ACpの生成
S238
Kcをコンテンツデータベースより取得
S240
トランザクションID、コンテンツID、Kc、ACmとACpをKPmc6にて暗号化し、
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6の生成
S242
S244へ

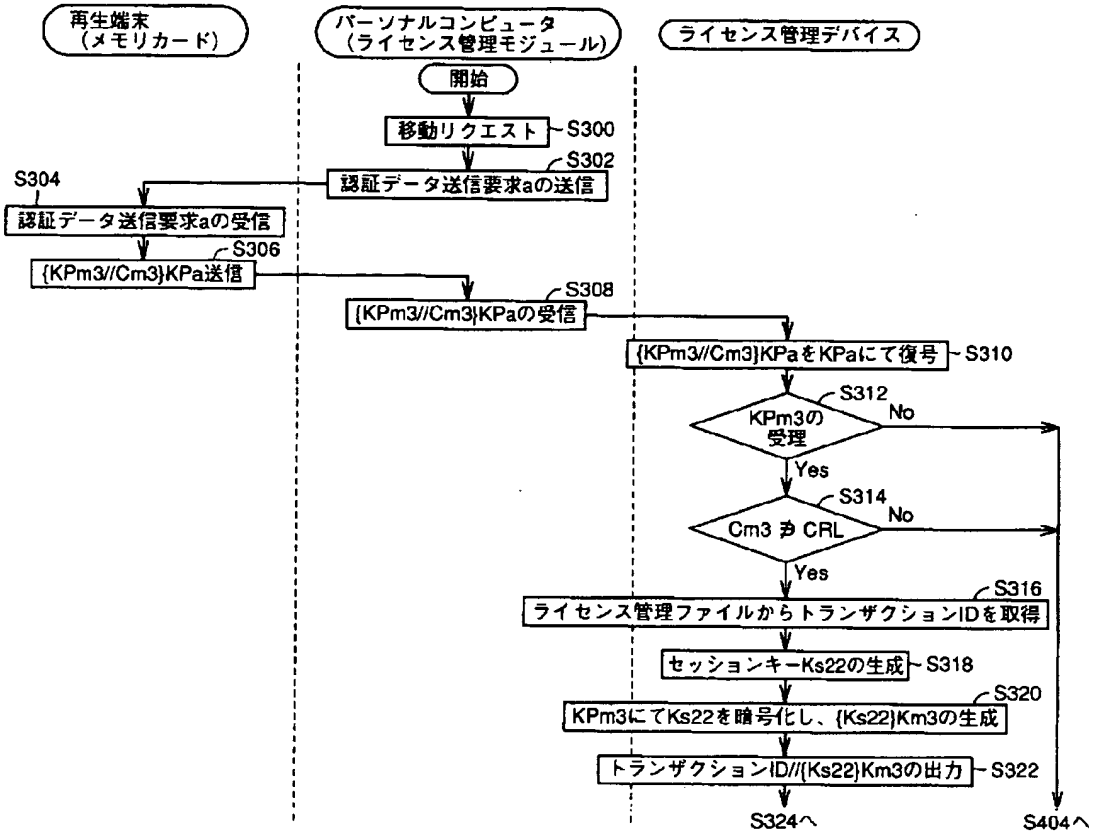
【図１６】


パーソナルコンピュータ
ライセンス管理モジュール
配信サーバ
S242から
S244
CRLdateは最新？
No
Yes
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}をKs2にて暗号化し、
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2の送信
S246
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2の受信
S248
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2にて復号
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6の受理
S250
CRLをCRLデータベースより取得し、差分CRLを生成
S252
差分CRLと{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}をKs2にて暗号化し、
{差分CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2の送信
S254
{差分CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2の受信
S256
{差分CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2にて復号
差分CRLと{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6の受理
S258
HDD内のCRLに受理した差分CRLを加え、
独自の暗号処理を施し、HDD内のCRLを書き換える
S260
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6をKmc6にて復号
{トランザクションID、コンテンツID、Kc、ACmおよびACpの受理
S262
S264へ

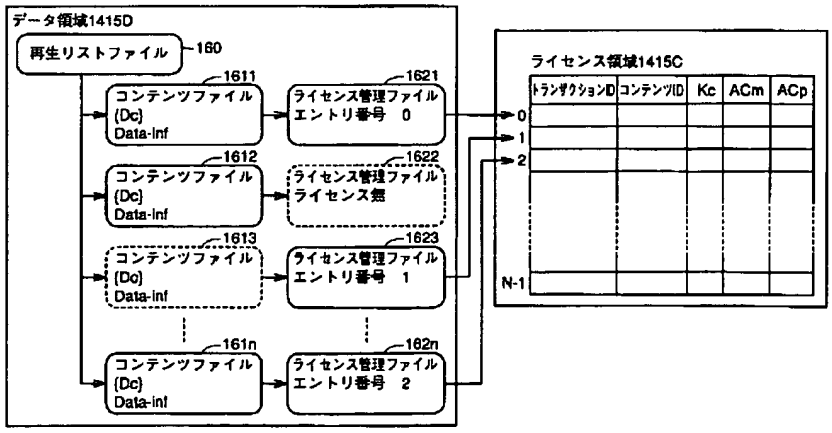
【図17】


パーソナルコンピュータ
ライセンス管理モジュール
S262から
チェックアウト可能数を初期値(=3)を含むチェックアウト情報を生成
S264
受理したトランザクションID、コンテンツID、Kc、ACm、ACpおよびチェックアウト情報に
独自の暗号処理を施した暗号化レベル1ライセンスを生成
S266
トランザクションIDとコンテンツ配信要求の送信
S268
配信サーバ
トランザクションID//コンテンツ配信要求の受信
S270
{Dc}KcとDc-infをコンテンツデータベースより取得し、
{Dc}Kc//Dc-infを送信
S272
{Dc}Kc//Dc-infの受信
{Dc}KcとDc-infの受理
S274
{Dc}KcとDc-infをコンテンツファイルとしてHDDに記録
S276
暗号化レベル1拡張ライセンスおよび平文のトランザクションIDおよびコンテンツIDを含む、
記録した{Dc}KcとDc-infに対するライセンス管理ファイルを生成し、HDDに記録
S278
HDDに記録されているコンテンツリストファイルに
受理したコンテンツの情報を追記
S280
トランザクションID//配信受理を送信
S282
S210 or S212から
トランザクションID//配信受理を受信
S284
課金処理
(課金情報を課金データベースに記録)
S286
終了
S288

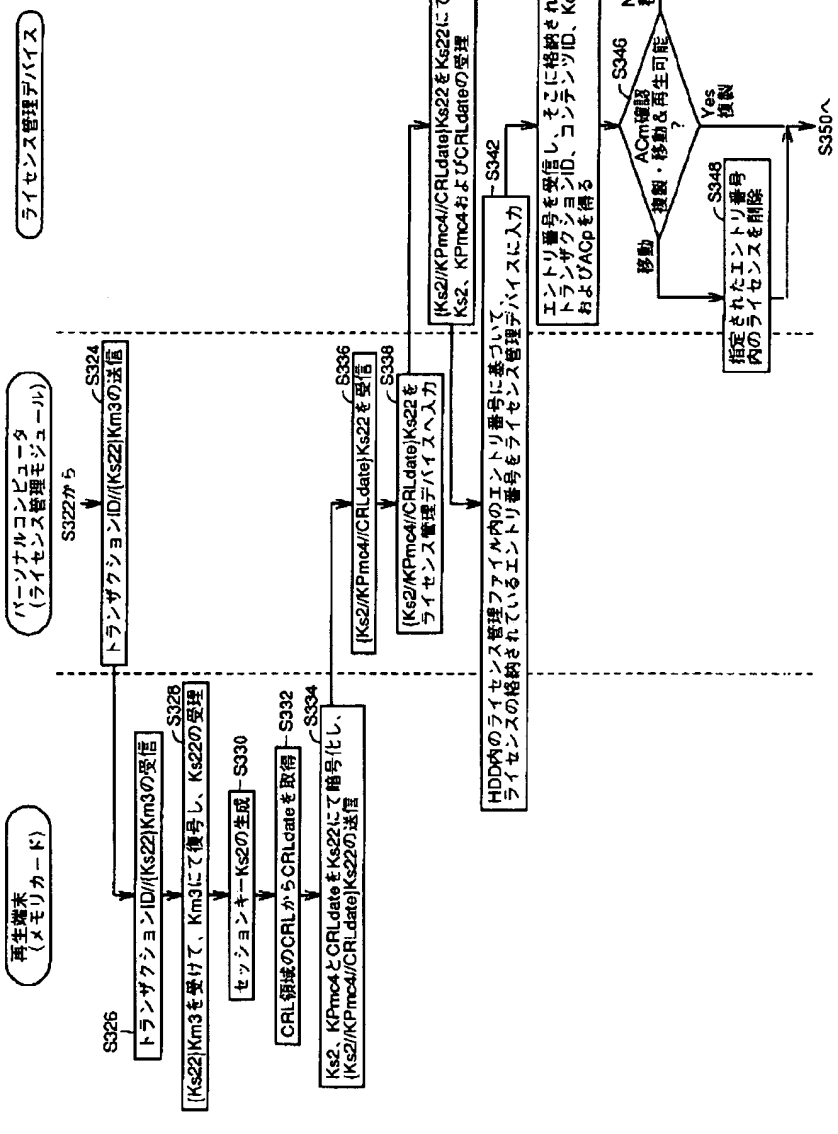
【図１８】


再生端末
（メモリカード）
パーソナルコンピュータ
（ライセンス管理モジュール）
ライセンス管理デバイス
開始
移動リクエスト
S300
S302
認証データ送信要求aの送信
S304
認証データ送信要求aの受信
S306
{KPm3//Cm3}KPa送信
S308
{KPm3//Cm3}KPaの受信
{KPm3//Cm3}KPaをKPaにて復号
S310
S312
KPm3の受理
No
Yes
S314
Cm3 ∌ CRL
No
Yes
S316
ライセンス管理ファイルからトランザクションIDを取得
セッションキーKs22の生成
S318
S320
KPm3にてKs22を暗号化し、{Ks22}Km3の生成
トランザクションID//{Ks22}Km3の出力
S322
S324へ
S404へ

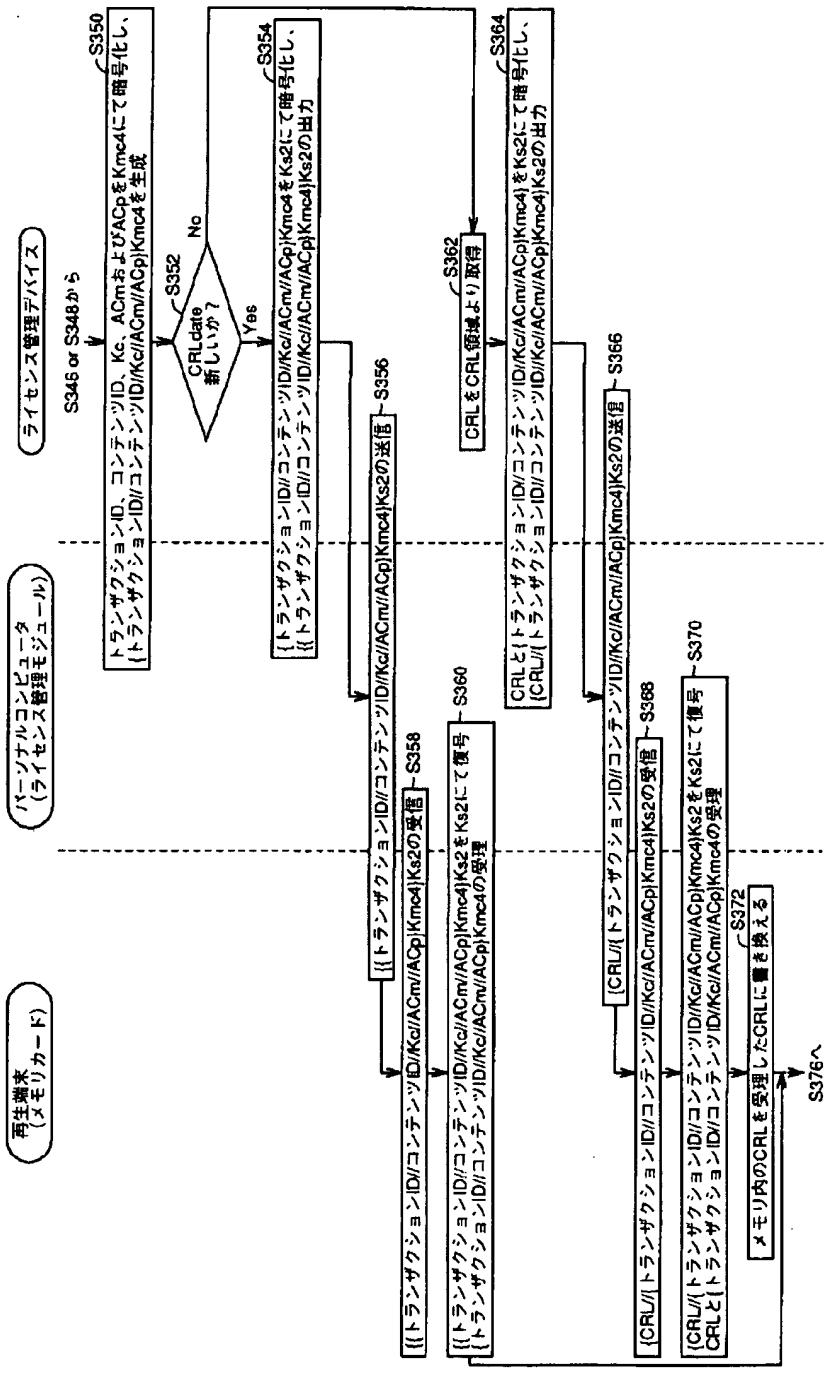
【図３２】


データ領域1415D
再生リストファイル
160
1611
コンテンツファイル
{Dc}
Data-Inf
1621
ライセンス管理ファイル
エントリ番号 0
1612
コンテンツファイル
{Dc}
Data-Inf
1622
ライセンス管理ファイル
ライセンス無
1613
コンテンツファイル
{Dc}
Data-Inf
1623
ライセンス管理ファイル
エントリ番号 1
161n
コンテンツファイル
{Dc}
Data-Inf
162n
ライセンス管理ファイル
エントリ番号 2
ライセンス領域1415C
トランザクションID
コンテンツID
Kc
ACm
ACp
0
1
2
N-1

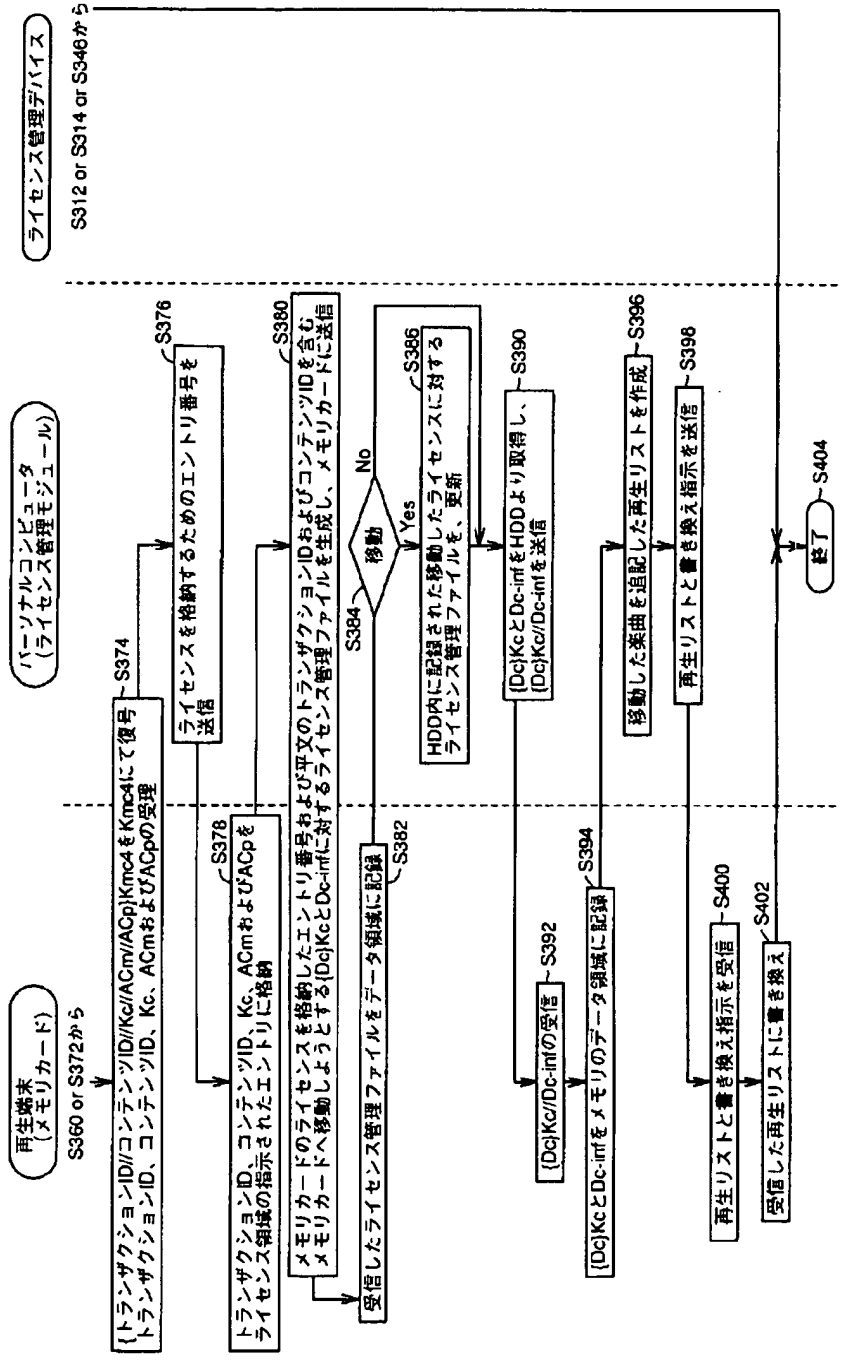
【図19】


再生端末
(メモリカード)
パーソナルコンピュータ
(ライセンス管理モジュール)
ライセンス管理デバイス
S322から
S324
トランザクションID//(Ks22|Km3)の送信
S326
トランザクションID//(Ks22|Km3)の受信
(Ks22|Km3を受け取り、Km3にて復号し、Ks22の受理
S326
セッションキーKs2の生成
S330
CRL領域のCRLからCRLdateを取得
S332
Ks2、KPmc4とCRLdateをKs22にて暗号化し、
(Ks2//KPmc4//CRLdate)Ks22の送信
S334
(Ks2//KPmc4//CRLdate)Ks22を受信
S336
(Ks2//KPmc4//CRLdate)Ks22を
ライセンス管理デバイスへ入力
S338
(Ks2//KPmc4//CRLdate)Ks22をKs22にて復号し、
Ks2、KPmc4およびCRLdateの受理
S340
HDD内のライセンス管理ファイル内のエントリ番号に基づいて
ライセンスの格納されているエントリ番号をライセンス管理デバイスに入力
S342
エントリ番号を受信し、そこに格納されている
トランザクションID、コンテンツID、Kc、ACm
およびACpを得る
S344
ACm確認
複製・移動&再生可能
?
S346
移動
No
移動・複製
Yes
複製
S348
指定されたエントリ番号
内のライセンスを削除
S404へ
S350へ

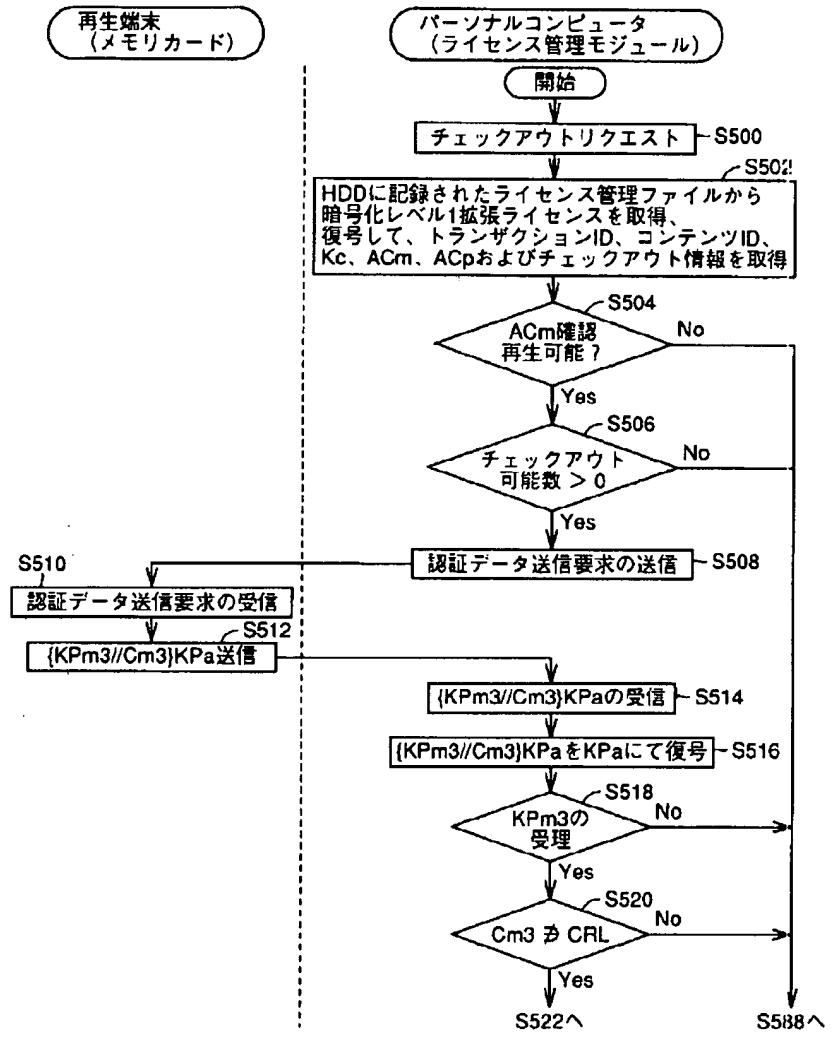
【図２０】


再生端末
(メモリカード)
パーソナルコンピュータ
(ライセンス管理モジュール)
ライセンス管理デバイス
S346 or S348から
S350
トランザクションID、コンテンツID、Kc、ACmおよびACpをKmc4にて暗号化し、
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4を生成
S352
CRLdate
新しいか？
No
Yes
S354
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4をKs2にて暗号化し、
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の出力
S356
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の送信
S358
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の受信
S360
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2にて復号
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4の受理
S362
CRLをCRL領域より取得
S364
CRLと{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4)をKs2にて暗号化し、
{CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の出力
S366
{CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の送信
S368
{CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の受信
S370
{CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2をKs2にて復号
CRLと{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4の受理
S372
メモリ内のCRLを受理したCRLに書き換える
S376へ

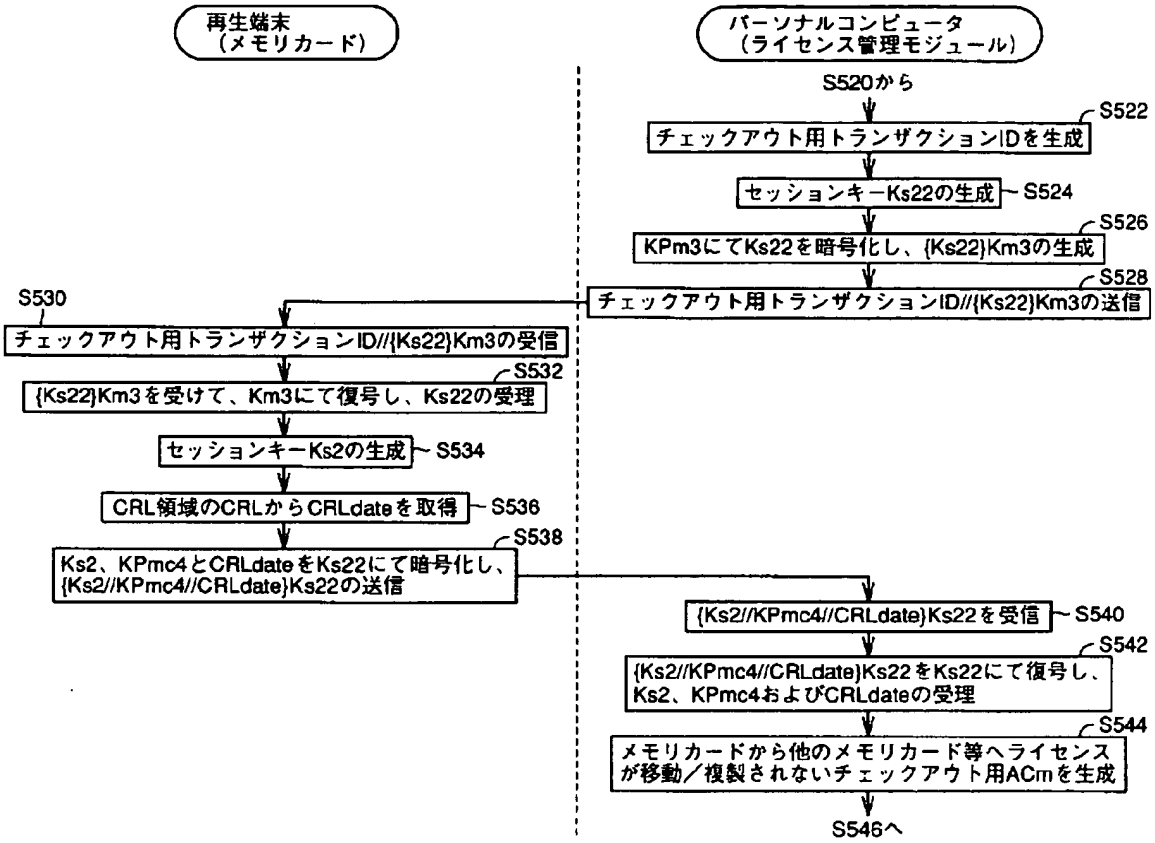
【図２１】


再生端末
(メモリカード)
パーソナルコンピュータ
(ライセンス管理モジュール)
ライセンス管理デバイス
S360 or S372から
S312 or S314 or S346から
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4をKmc4にて復号
トランザクションID、コンテンツID、Kc、ACmおよびACpの受理
S374
ライセンスを格納するためのエントリ番号を送信
S376
トランザクションID、コンテンツID、Kc、ACmおよびACpをライセンス領域の指示されたエントリに格納
S378
メモリカードのライセンスを格納したエントリ番号および平文のトランザクションIDおよびコンテンツIDを含むメモリカードへ移動しようとする{Dc}KcとDc-infに対するライセンス管理ファイルを生成し、メモリカードに送信
S380
S384
移動
No
Yes
S386
HDD内に記録された移動したライセンスに対するライセンス管理ファイルも、更新
受信したライセンス管理ファイルをデータ領域に記録
S382
{Dc}Kc//Dc-infの受信
S392
{Dc}KcとDc-infをHDDより取得し、{Dc}Kc//Dc-infを送信
S390
{Dc}KcとDc-infをメモリのデータ領域に記録
S394
移動した楽曲を追記した再生リストを作成
S396
再生リストと書き換え指示を送信
S398
再生リストと書き換え指示を受信
S400
受信した再生リストに書き換え
S402
終了
S404

【図２２】


再生端末
（メモリカード）
パーソナルコンピュータ
（ライセンス管理モジュール）
開始
チェックアウトリクエスト
S500
S502
HDDに記録されたライセンス管理ファイルから
暗号化レベル1拡張ライセンスを取得、
復号して、トランザクションID、コンテンツID、
Kc、ACm、ACpおよびチェックアウト情報を取得
S504
ACm確認
再生可能？
No
Yes
S506
チェックアウト
可能数＞0
No
Yes
認証データ送信要求の送信
S508
S510
認証データ送信要求の受信
S512
{KPm3//Cm3}KPa送信
{KPm3//Cm3}KPaの受信
S514
{KPm3//Cm3}KPaをKPaにて復号
S516
S518
KPm3の
受理
No
Yes
S520
Cm3 ∌ CRL
No
Yes
S522へ
S538へ

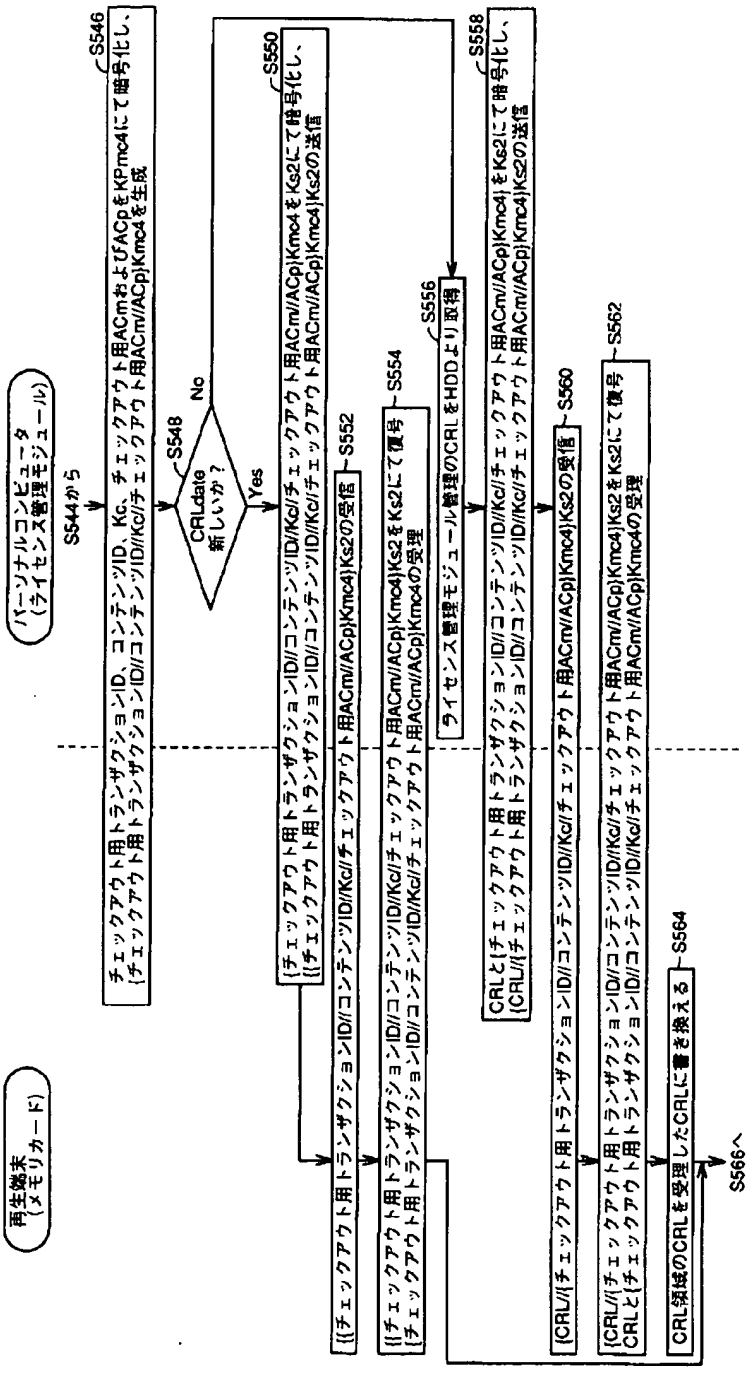
【図２３】



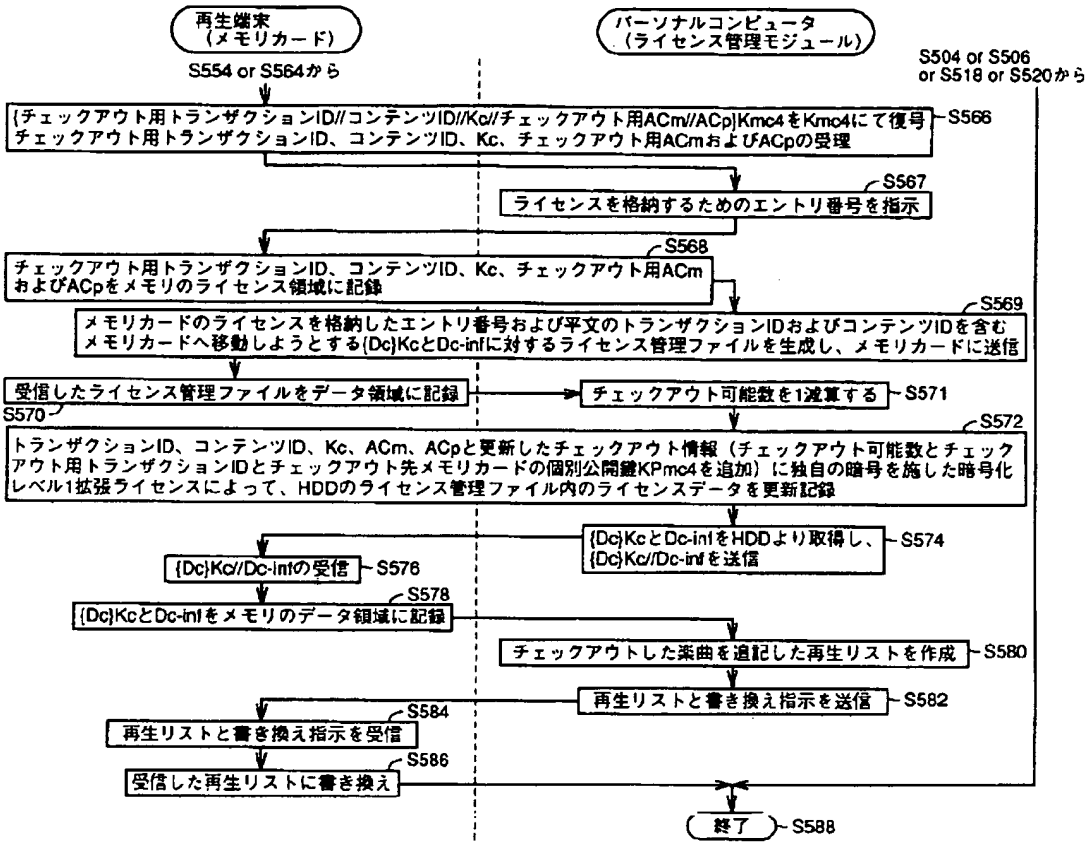
【図３７】

ACm	
Play_count	再生可能回数（１バイト） 0　：再生不可 1～254　：再生可能回数 再生許諾毎に１減じる。 255　：無制限
Move_count	移動・複製制御（１バイト） 0　：移動・複製不可 1～15　：移動不可・複製可（制限付き） 複製可能な世代を示す。複製毎に１減ずる。 17 ～239　：未使用 240～253　：移動可・複製可（制限付き） 254-Move_countが複製可能な世代を示す。複製毎に１増やす。 254　：移動可・複製不可 255　：移動・複製可（無制限）
Safe_Level	ライセンスの保護レベル（１バイト） メモカード＝再生端末　＞　インポートコンテンツ
ACp	
flags(0) flags(1) flags(2) +Play_length flags(3) + not_after flags(4) + not_before flags(5) + Region_code	再生速度変換可否 編集可否 再生可能サイズ（部分再生） 利用終了日時 利用開始日時 地域コード
チェックアウト可能数 checkout_count	チェックアウト可能なライセンス数（１バイト） 0　：チェックアウト不可 1～　：チェックアウト可能ライセンス数 チェックアウト毎に１減じ，チェックイン毎に１増やす。

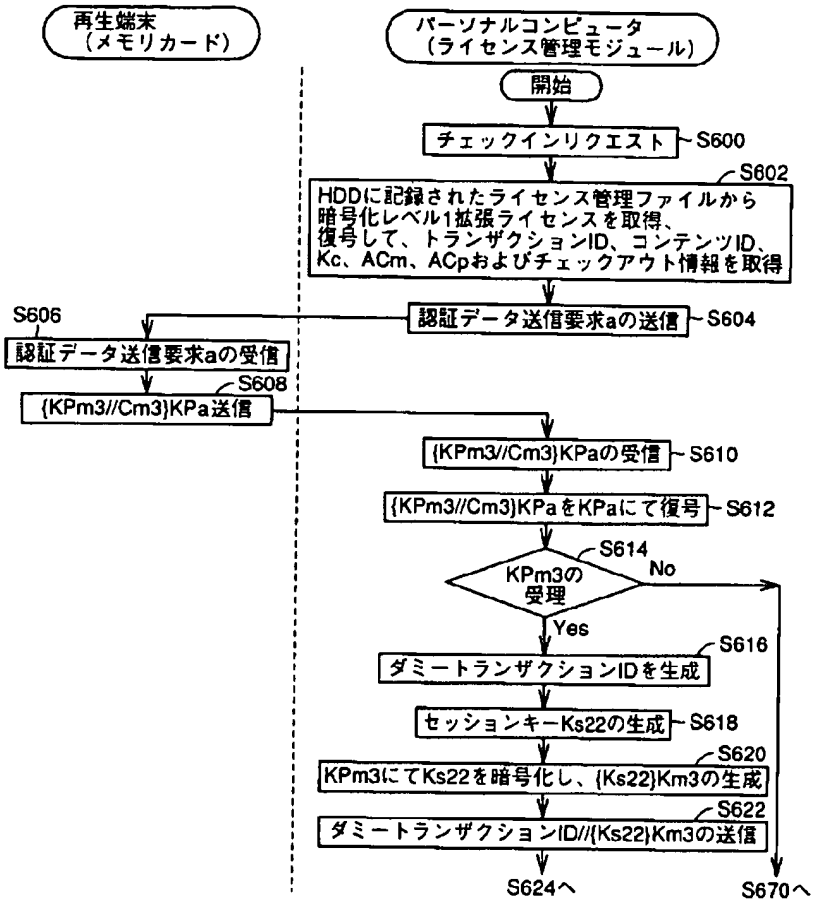
【図２４】


再生端末
(メモリカード)
パーソナルコンピュータ
(ライセンス管理モジュール)
S544から
S546
チェックアウト用トランザクションID、コンテンツID、Kc、チェックアウト用ACmおよびACpをKPmc4にて暗号化し、
{チェックアウト用トランザクションID//Kc//チェックアウト用ACm//ACp}Kmc4を生成
S548
CRLdate
新しいか？
No
Yes
S550
{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4をKs2にて暗号化し、
{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2の送信
S552
{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2の受信
S554
{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2にて復号
{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}の受理
S556
ライセンス管理モジュールCRLをHDDより取得
S558
CRLと{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}をKs2にて暗号化し、
{CRL//{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2の送信
S560
{CRL//{チェックアウト用トランザクションID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2の受信
S562
{CRL//{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2にて復号
CRLと{{チェックアウト用トランザクションID//Kc//チェックアウト用ACm//ACp}Kmc4}の受理
S564
CRL領域のCRLを受理したCRLに書き換える
S566へ

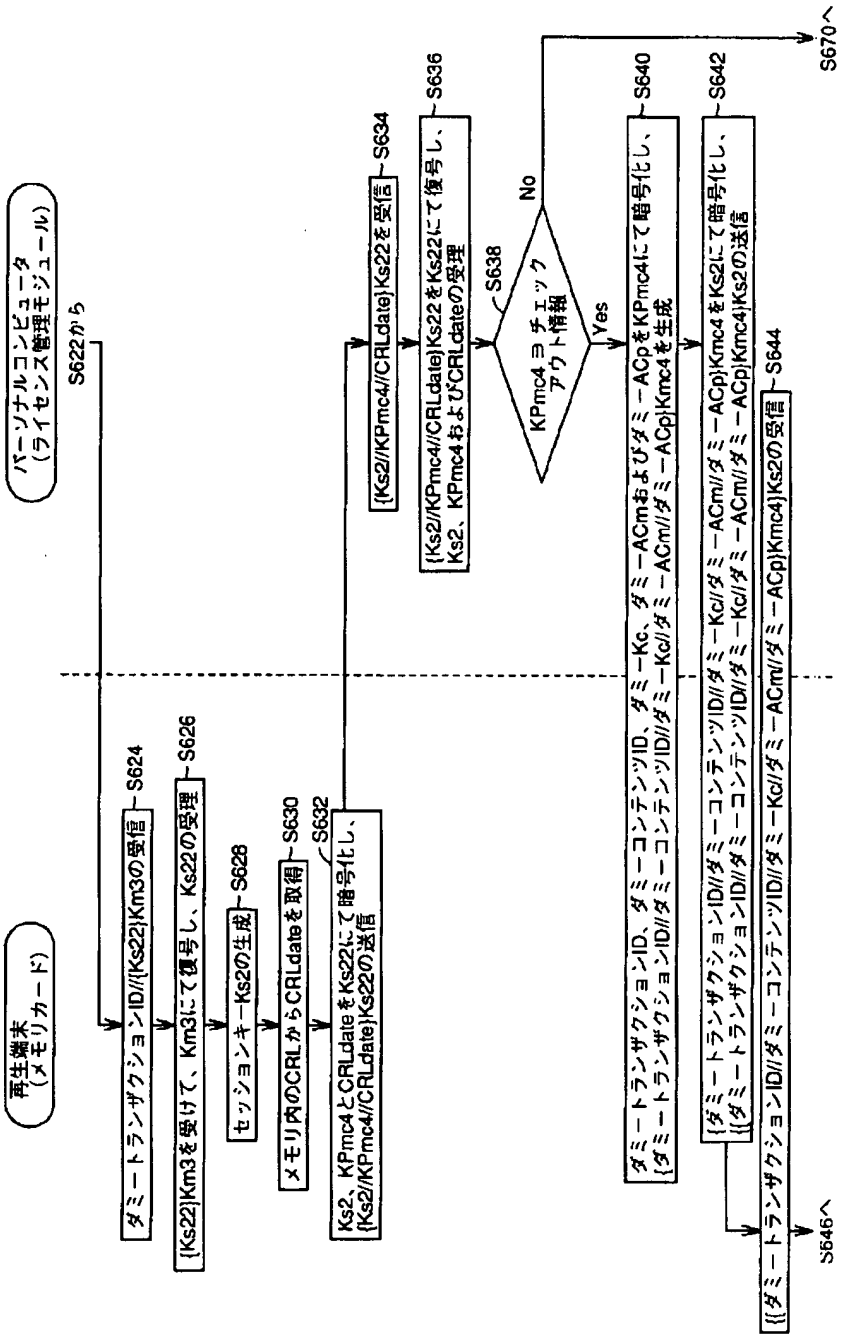
【図２５】


再生端末
（メモリカード）
パーソナルコンピュータ
（ライセンス管理モジュール）
S554 or S564から
S504 or S506
or S518 or S520から
{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4をKmc4にて復号
チェックアウト用トランザクションID、コンテンツID、Kc、チェックアウト用ACmおよびACpの受理
S566
ライセンスを格納するためのエントリ番号を指示
S567
チェックアウト用トランザクションID、コンテンツID、Kc、チェックアウト用ACm
およびACpをメモリのライセンス領域に記録
S568
メモリカードのライセンスを格納したエントリ番号および平文のトランザクションIDおよびコンテンツIDを含む
メモリカードへ移動しようとする{Dc}KcとDc-infに対するライセンス管理ファイルを生成し、メモリカードに送信
S569
受信したライセンス管理ファイルをデータ領域に記録
S570
チェックアウト可能数を1減算する
S571
トランザクションID、コンテンツID、Kc、ACm、ACpと更新したチェックアウト情報（チェックアウト可能数とチェック
アウト用トランザクションIDとチェックアウト先メモリカードの個別公開鍵KPmc4を追加）に独自の暗号を施した暗号化
レベル1拡張ライセンスによって、HDDのライセンス管理ファイル内のライセンスデータを更新記録
S572
{Dc}KcとDc-infをHDDより取得し、
{Dc}Kc//Dc-infを送信
S574
{Dc}Kc//Dc-infの受信
S576
{Dc}KcとDc-infをメモリのデータ領域に記録
S578
チェックアウトした楽曲を追記した再生リストを作成
S580
再生リストと書き換え指示を送信
S582
再生リストと書き換え指示を受信
S584
受信した再生リストに書き換え
S586
終了
S588

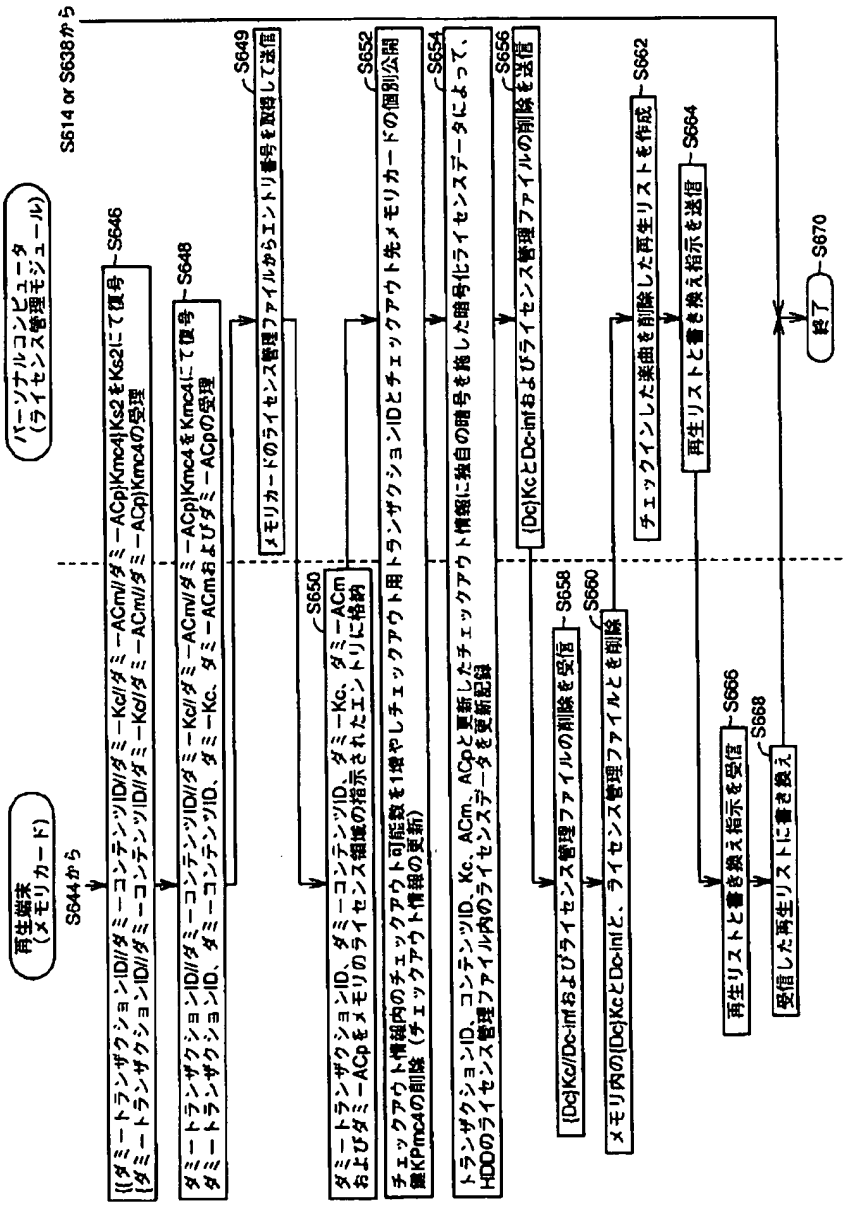
【図２６】


再生端末
（メモリカード）
パーソナルコンピュータ
（ライセンス管理モジュール）
開始
チェックインリクエスト
S600
S602
HDDに記録されたライセンス管理ファイルから
暗号化レベル1拡張ライセンスを取得、
復号して、トランザクションID、コンテンツID、
Kc、ACm、ACpおよびチェックアウト情報を取得
認証データ送信要求aの送信
S604
S606
認証データ送信要求aの受信
S608
{KPm3//Cm3}KPa送信
{KPm3//Cm3}KPaの受信
S610
{KPm3//Cm3}KPaをKPaにて復号
S612
S614
KPm3の
受理
No
Yes
S616
ダミートランザクションIDを生成
セッションキーKs22の生成
S618
S620
KPm3にてKs22を暗号化し、{Ks22}Km3の生成
S622
ダミートランザクションID//{Ks22}Km3の送信
S624へ
S670へ

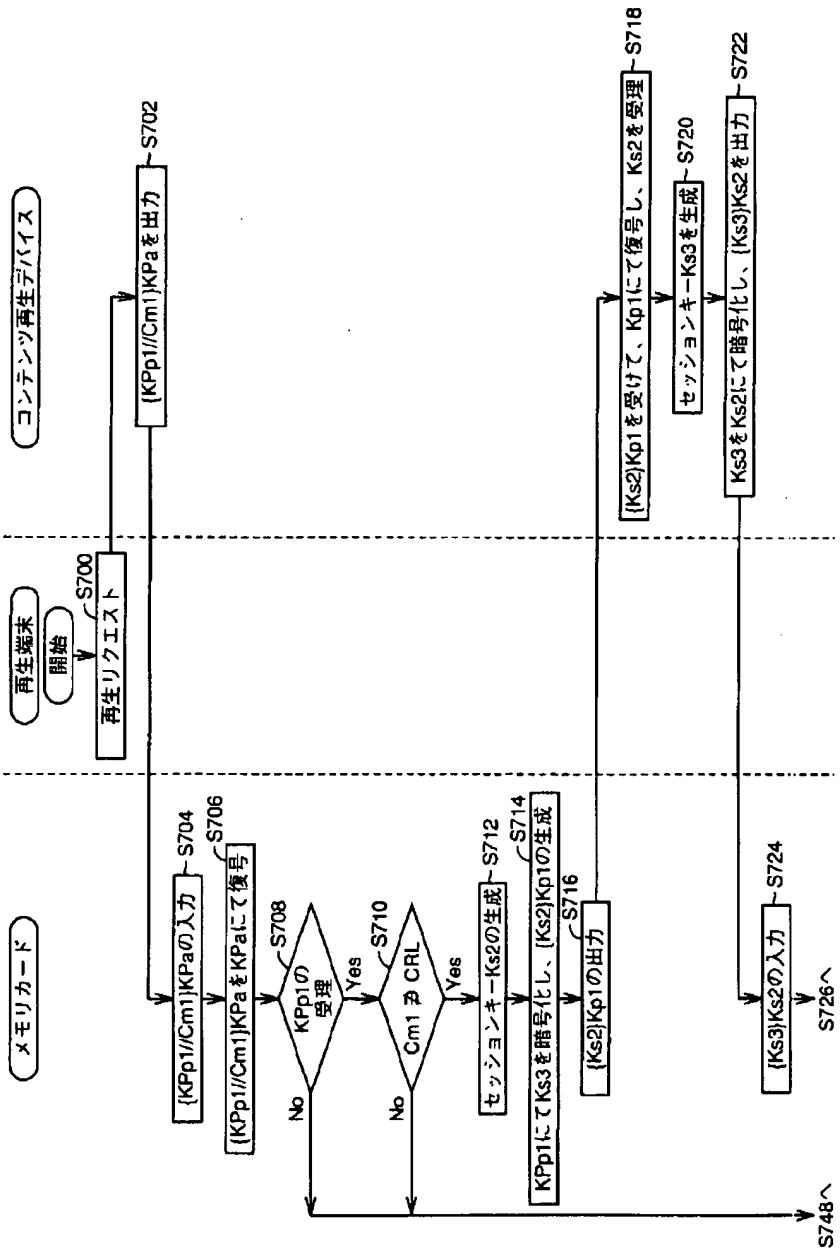
【図２７】


再生端末
(メモリカード)
パーソナルコンピュータ
(ライセンス管理モジュール)
S622から
ダミートランザクションID//{Ks22}Km3の受信
S624
{Ks22}Km3を受けて、Km3にて復号し、Ks22の受理
S626
セッションキーKs2の生成
S628
メモリ内のCRLからCRLdateを取得
S630
Ks2、KPmc4とCRLdateをKs22にて暗号化し、
{Ks2//KPmc4//CRLdate}Ks22の送信
S632
{Ks2//KPmc4//CRLdate}Ks22を受信
S634
{Ks2//KPmc4//CRLdate}Ks22をKs22にて復号し、
Ks2、KPmc4およびCRLdateの受理
S636
KPmc4ヨリチェック
アウト情報
S638
No
Yes
ダミートランザクションID、ダミーコンテンツID、ダミーKc、ダミーACmおよびダミーACpをKPmc4にて暗号化し、
{ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp}Kmc4を生成
S640
{ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp}Kmc4をKs2にて暗号化し、
{{ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp}Kmc4}Ks2の送信
S642
{{ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp}Kmc4}Ks2の受信
S644
S646へ
S670へ

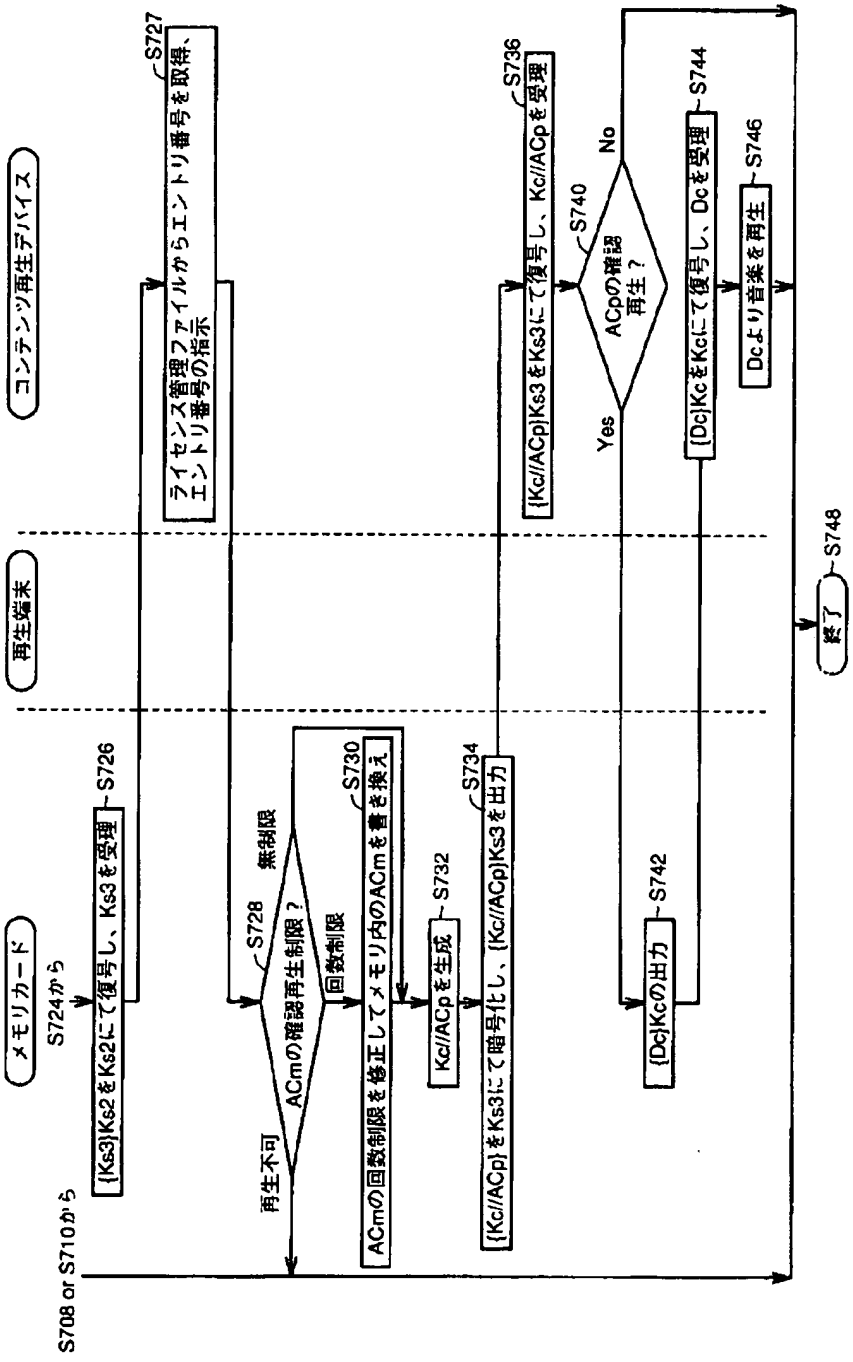
【図２８】


再生端末
(メモリカード)
S644から
パーソナルコンピュータ
(ライセンス管理モジュール)
S614 or S638から
{(ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp)Kmc4}Ks2をKs2にて復号
S646
(ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp)Kmc4の受理
ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp)Kmc4をKmc4にて復号
S648
ダミートランザクションID、ダミーコンテンツID、ダミーKc、ダミーACmおよびダミーACpの受理
メモリカードのライセンス管理ファイルからエントリ番号を取得して送信
S649
S650
ダミートランザクションID、ダミーコンテンツID、ダミーKc、ダミーACm
およびダミーACpをメモリのライセンス領域の指示されたエントリに格納
S652
チェックアウト情報内のチェックアウト可能数を1増やしチェックアウト用トランザクションIDとチェックアウト先メモリカードの個別公開
鍵KPmc4の削除（チェックアウト情報の更新）
S654
トランザクションID、コンテンツID、Kc、ACm、ACpと更新したチェックアウト情報に独自の暗号を施した暗号化ライセンスデータによって、
HDDのライセンス管理ファイル内のライセンスデータを更新記録
S656
{Dc}KcとDc-infおよびライセンス管理ファイルの削除を送信
{Dc}Kc//Dc-infおよびライセンス管理ファイルの削除を受信
S658
メモリ内の{Dc}KcとDc-infと、ライセンス管理ファイルとを削除
S660
チェックインした楽曲を削除した再生リストを作成
S662
再生リストと書き換え指示を送信
S664
再生リストと書き換え指示を受信
S666
受信した再生リストに書き換え
S668
終了
S670

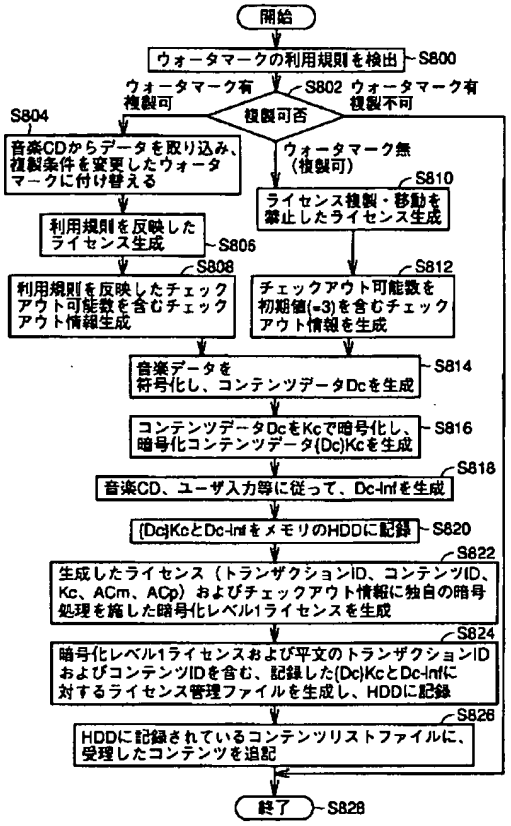
【図２９】


コンテンツ再生デバイス
再生端末
メモリカード
開始
S700
再生リクエスト
S702
{KPp1//Cm1}KPaを出力
S704
{KPp1//Cm1}KPaの入力
S706
{KPp1//Cm1}KPaをKPaにて復号
S708
KPp1の受理
No
Yes
S710
Cm1 ≠ CRL
No
Yes
S712
セッションキーKs2の生成
S714
KPp1にてKs3を暗号化し、{Ks2}Kp1の生成
S716
{Ks2}Kp1の出力
S718
{Ks2}Kp1を受けて、Kp1にて復号し、Ks2を受理
S720
セッションキーKs3を生成
S722
Ks3をKs2にて暗号化し、{Ks3}Ks2を出力
S724
{Ks3}Ks2の入力
S726へ
S748へ

【図30】


メモリカード
再生端末
コンテンツ再生デバイス
S708 or S710から
S724から
{Ks3}Ks2をKs2にて復号し、Ks3を受理
S726
ライセンス管理ファイルからエントリ番号を取得、エントリ番号の指示
S727
S728
ACmの確認再生制限？
再生不可
無制限
回数制限
S730
ACmの回数制限を修正してメモリ内のACmを書き換え
Kc//ACpを生成
S732
{Kc//ACp}をKs3にて暗号化し、{Kc//ACp}Ks3を出力
S734
{Kc//ACp}Ks3をKs3にて復号し、Kc//ACpを受理
S736
S740
ACpの確認再生？
Yes
No
{Dc}Kcの出力
S742
{Dc}KcをKcにて復号し、Dcを受理
S744
Dcより音楽を再生
S746
終了
S748

【図３４】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I		ﾃｰﾏｺｰﾄﾞ（参考）
G１０K　15/02		G１１B　20/10	H	
G１１B　20/10		H０４L　9/00	６０１B	
H０４L　9/32			６７５B	

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(71)出願人　000004167
日本コロムビア株式会社
東京都港区赤坂４丁目14番14号
(72)発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72)発明者　上村　透
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72)発明者　宮園　真也
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72)発明者　畠山　卓久
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　高橋　政孝
石川県河北郡宇ノ気町字宇野気ヌ98番地の２　株式会社ピーエフユー内
(72)発明者　常広　隆司
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所システム開発研究所横浜ラボラトリ内

(72)発明者　大森　良夫
神奈川県川崎市川崎区港町５番１号　日本
コロムビア株式会社川崎工場内

Ｆターム(参考)　5D044 AB05 AB07 BC01 BC04 CC04
CC08 DE22 DE28 DE50 EF05
FG18 GK08 GK12 GK17 HL02
HL08 HL11
5J104 AA07 AA14 AA16 AA37 EA01
EA05 EA06 EA22 JA21 KA02
KA05 NA02 NA33 NA36 NA37

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-164879**

(43)Date of publication of application : **07.06.2002**

(51)Int.Cl. H04L 9/08
G06F 13/00
G06F 17/60
G09C 5/00
G10K 15/02
G11B 20/10
H04L 9/32

(21)Application number : **2000-361631**

(22)Date of filing : **28.11.2000**

(71)Applicant : **SANYO ELECTRIC CO LTD**
FUJITSU LTD
PFU LTD
HITACHI LTD
NIPPON COLUMBIA CO LTD

(72)Inventor : **HORI YOSHIHIRO**
KAMIMURA TORU
MIYAZONO SHINYA
HATAKEYAMA TAKAHISA
TAKAHASHI MASATAKA
TSUNEHIRO TAKASHI
OMORI YOSHIO

(54) DATA TERMINAL DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data terminal device capable of ripping contents data off in response to regularity in the usage rules of contents data.

SOLUTION: A watermark detection means 5400 detects a watermark from music data, and a watermark decision means 5401 decides whether the usage rule of the detected watermark has any regularity. A license generation means 5403 generates a license according to the regularity in the usage rules for the watermark. A remark means 5402 replaces the watermark with the one of which the copying condition for musical data is changed according to the regularity in the usage rules for the watermark. A music encoder 5404 encodes music data from the remark means 5402 to a prescribed method. A cipher means 5405 encrypts music data from the music encoder 5404 by the license

key generated at the license generation means 5403.

CLAIMS

[Claim(s)]
[Claim 1]Enciphered content data which acquired contents data of a plaintext and enciphered said contents data, It is a Data Terminal Equipment which generates a local license for decoding said enciphered content data and reproducing, Said local license is generated based on duplicate propriety information included in said contents data, An enciphered content creating means which enciphers said contents data and generates said enciphered content data with a license key contained in the generated local license, A cipher-processing means to generate an encryption local license which gave encryption original with said generated local license, A Data Terminal Equipment which it has a memory measure which memorizes said encryption local license and enciphered content data, and a control section, and said control section gives said acquired contents data to said enciphered content creating means, and gives said local license to said cipher-processing means.
[Claim 2]Enciphered content data which enciphered contents data, and a license for decoding said enciphered content data and reproducing are received from a distributing server, And/or, it is a Data Terminal Equipment which generates a local license for acquiring said contents data, decoding said enciphered content data and said enciphered content data, and reproducing, A license management device which performs mutual recognition between said distributing servers, and receives said enciphered content data and said license from said distributing server, and holds said license, Said local license is generated based on duplicate propriety information included in said contents data, An enciphered content creating means which enciphers said contents data and generates said enciphered content data with a license key contained in the generated local license, Have a cipher-processing means to generate an encryption local license which gave encryption original with said generated local license, a memory measure which memorizes said license, said encryption local license, and said enciphered content data, and a control section, and said control section, A Data Terminal Equipment which gives said acquired contents data to said enciphered content creating means, and gives said local license to said cipher-processing means.
[Claim 3]Enciphered content data which enciphered contents data, and a license for decoding said enciphered content data and reproducing are received from a distributing server, And/or, are a local license for acquiring said contents data, decoding said enciphered content data and said enciphered content data, and reproducing a Data Terminal Equipment to generate, and by software. A license management module which performs mutual recognition between said distributing servers, and receives said enciphered content data and said license from said distributing server, Said local license is generated based on duplicate propriety information included in said contents data, An enciphered content creating means which enciphers said contents data and generates said enciphered content data with a license key contained in the generated local license, A cipher-processing means to generate an encryption license which gave encryption original with an encryption local license which gave encryption original with said generated local license, or said received license, A memory measure which memorizes said encryption license, said encryption local license, and said enciphered content data, A Data Terminal Equipment which it has a control section, and said control section gives said acquired contents data to said enciphered content creating means, and gives said local license and said license to said cipher-processing means.

[Claim 4]Enciphered content data which enciphered contents data, and a license for decoding said enciphered content data and reproducing are received from a distributing server, And/or, it is a Data Terminal Equipment which generates a local license for acquiring said contents data, decoding said enciphered content data and said enciphered content data, and reproducing, By a license management device which performs mutual recognition between said distributing servers, and receives said enciphered content data and said license from said distributing server, and holds said license, and software. A license management module which performs mutual recognition between said distributing servers, and receives said enciphered content data and said license from said distributing server, Said local license is generated based on duplicate propriety information included in said contents data, An enciphered content creating means which enciphers said contents data and generates said enciphered content data with a license key contained in the generated local license, and an encryption local license which gave encryption original with said generated local license, Or a cipher-processing means to generate an encryption license which gave encryption original with a license received with said license management module, Have a memory measure which memorizes said encryption license, said encryption local license, and said enciphered content data, and a control section, and said control section, A Data Terminal Equipment which gives said acquired contents data to said enciphered content creating means, and gives said license and said local license to said cipher-processing means.

[Claim 5]Said enciphered content creating means generates further a number for lending out said generated enciphered content data and a local license to other devices which can be lent out, and said cipher-processing means, A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 4 which gives encryption original with said local license and said number which can be lent out, and generates said encryption local license.

[Claim 6]Have further a file generating means to generate a license management file which includes said encryption local license at least, and said control section, A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 5 which gives said enciphered content data and said license management file to said memory measure.

[Claim 7]A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 6 in which said enciphered content creating means generates a local license reflecting said duplicate permit information when said duplicate propriety information is the duplicate permit information to which a duplicate is permitted.

[Claim 8]When said enciphered content creating means is duplicate permit information which said duplicate propriety information permits a duplicate, When a local license reflecting said duplicate permit information is generated and said contents data does not include said duplicate propriety information, A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 6 which generates a local license which forbade a duplicate and movement of a license for decoding said enciphered content data and reproducing.

[Claim 9]A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 8 which is further equipped with a medium driving means which drives a recording medium which recorded said contents data, and said control section gives contents data which said medium driving means read from said recording medium to said enciphered content creating means.

[Claim 10]A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 8 which gives contents data which said control section received by the Internet to said enciphered content creating means.

[Claim 11]A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 10 characterized by comprising the following.

A duplicate propriety information detection means in which said enciphered content creating means detects said duplicate propriety information from said contents data.
A duplicate propriety information judging means which judges said detected duplicate propriety information.
A license creating means which generates said local license based on a decision result of said duplicate propriety information judging means.
Cryptographer stage which enciphers said contents data with said license key.

[Claim 12]A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 10 characterized by comprising the following.
A duplicate propriety information detection means in which said enciphered content creating means detects said duplicate propriety information from said contents data.
A duplicate propriety information judging means which judges said detected duplicate propriety information.
A duplicate alteration-of-condition means which changes duplicate conditions based on a decision result of said duplicate propriety information judging means, and is written in said contents data.
An encoding means which codes contents data from said duplicate alteration-of-condition means to a prescribed method, A license creating means which generates said local license based on a decision result of said duplicate propriety information judging means, and a cryptographer stage which enciphers contents data coded by said prescribed method with said license key.

[Claim 13]The Data Terminal Equipment according to claim 12 which generates said local license, comprising:
A content identifier as which said license creating means specifies said enciphered content data.
A communication identifier which specifies communication when lending out said enciphered content data and said license to other devices.
Said license key.
A recorder access condition over a data recorder which records said enciphered content data and said local license, and a playback equipment access condition over a data reproduction apparatus which decodes said enciphered content data and is reproduced according to said license.

[Claim 14]Said content identifier and said communication identifier, Comprise a fixed area and a management domain following said fixed area, and said license creating means, A local signal which shows that said content identifier or said communication identifier was generated in a Data Terminal Equipment is written in said fixed area, The Data Terminal Equipment according to claim 13 which writes an identification number corresponding to said enciphered content data in said management domain, and generates a content identifier and a communication identifier.
[Claim 15]The Data Terminal Equipment according to claim 13 in which said license creating means generates said communication identifier and said license key by generating of a random number.
[Claim 16]The Data Terminal Equipment comprising according to claim 13:
The number of times of refreshable to which said recorder access condition expresses propriety and the number of times of possible of reproduction of said enciphered content data.
Move copy control information which controls movement and a duplicate of said enciphered content data and a local license.

Protecting level information showing a protecting level of said local license.

[Claim 17]The Data Terminal Equipment comprising according to claim 16:
The 1st number of times of refreshable that comprises a fixed value as which said number of times of refreshable expresses a reproduction failure of said enciphered content data.
The 2nd number of times of refreshable that comprises a variation which carries out monotone decreasing whenever it permits reproduction of said enciphered content data.
The 1st control information to which it changes from the 3rd number of times of refreshable that permits reproduction of said enciphered content data indefinitely and which said move copy control information forbids movement and a duplicate of said enciphered content data and said local license.
The 2nd control information that forbids movement of said enciphered content data and said local license, and permits a duplicate of said enciphered content data and said local license conditionally, The 3rd control information that permits movement and a duplicate of said enciphered content data and said local license conditionally, The 4th control information that permits movement of said enciphered content data and said local license, and forbids a duplicate of said enciphered content data and said local license, The 5th control information that permits indefinitely movement and a duplicate of said enciphered content data and said local license.

[Claim 18]Including a variation which carries out monotone decreasing of said 2nd control information for every duplicate of said enciphered content data and said local license, and expresses the number of times which can be reproduced, said 3rd control information, The Data Terminal Equipment according to claim 17 containing a variation which carries out a monotone increase for every movement and duplicate of said enciphered content data and said local license.
[Claim 19]The Data Terminal Equipment comprising according to claim 13:
The 1st signal with which said playback equipment access condition shows conversion propriety of reproduction speed of said enciphered content data.
The 2nd signal that shows propriety of edit of said enciphered content data.
The 3rd signal that shows size of refreshable enciphered content data.
The 4th signal that shows the time of the final day of use of said enciphered content data, the 5th signal that shows the time of a use opening day of said enciphered content data, and an area code.

[Claim 20]The Data Terminal Equipment comprising according to claim 13:
Inhibition information which said lending information forbids a loan of said enciphered content data and said local license.
Loan permit information which carries out monotone decreasing for every loan of said enciphered content data and said local license, and carries out a monotone increase for every return of said enciphered content data and said local license.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the Data Terminal Equipment used in the data distribution system which makes copyright protection to the copied information

possible.
[0002]
[Description of the Prior Art]Each user is able to access network information easily in recent years with the terminal for the individuals [progress / of information-and-telecommunications networks, such as the Internet, etc.] using a portable telephone etc.
[0003]In such an information-and-telecommunications network, information is transmitted by a digital signal. Therefore, it is possible to perform a copy of data, without producing most degradation of the tone quality by such a copy, or image quality, even when an individual user copies the music and picture image data which were transmitted, for example in the above information-and-telecommunications networks.
[0004]Therefore, if the policy for suitable copyright protection is not taken when the creation thing in which the right of authors, such as music data and image data, exists in such an information-and-telecommunications screen oversize is transmitted, there is a possibility of infringing on right of an owner of a copyright remarkably.
[0005]On the other hand, supposing it cannot give top priority to the purpose of copyright protection and cannot distribute work data via the digital information communications network to expand rapidly, it will become rather disadvantageous also for the owner of a copyright who can collect a fixed royalty when reproducing work data fundamentally.
[0006]If it thinks and sees here not taking the case of distribution through the above digital information communications networks but taking the case of the recording medium which recorded digital data, Usually, about CD (compact disk) which recorded the music data currently sold, the copy of the music data from CD to magneto-optical discs (MD etc.) can be freely performed in principle, as long as the copied music concerned is stopped to individual use. However, the individual user who performs digital sound recording etc. is to pay an owner of a copyright indirectly the constant sum of the prices for media, such as digital-sound-recording apparatus itself and MD, as guarantee money.
[0007]And when the music data which is a digital signal is copied to MD from CD, It has come to be unable to perform copying music information to MD of further others as digital data from recordable MD on the composition of apparatus in view of these information being the digital data which does not almost have copy degradation for copyright protection.
[0008]Since distributing music data and image data to the public through a digital information communications network also from such a situation is an act from which itself receives restriction by rights of public transmission of an owner of a copyright, sufficient policy for copyright protection needs to be devised.
[0009]In this case, it is necessary for the contents data received once to prevent being reproduced still more freely about the contents data of music data, image data, etc. which is works transmitted to the public through an information-and-telecommunications network.
[0010]Then, the data distribution system with which the distributing server holding the enciphered content data which enciphered contents data distributes enciphered content data via a terminal unit to the memory card with which terminal units, such as a portable telephone, were equipped is proposed. In this data distribution system, the open encryption key and certificate of the memory card beforehand attested by the certificate authority are transmitted to a distributing server in the case of the distribution request of enciphered content data, After checking having received the certificate in which the distributing server was attested, the license key for decoding enciphered content data and enciphered content data to a memory card is transmitted. And when distributing

enciphered content data and a license key, a distributing server and a memory card generate a different session key for every distribution, with the generated session key, encipher an open encryption key and exchange keys a distributing server and between memory cards.
[0011]Eventually, a distributing server transmits the license which it was enciphered with the open encryption key of memory card each, and was further enciphered with the session key, and enciphered content data to a memory card. And a memory card records the license key and enciphered content data which were received on a memory card.
[0012]And a cellular phone is equipped with a memory card when reproducing the enciphered content data recorded on the memory card. A cellular phone also has a dedicated communication circuit for decoding the enciphered content data from a memory card other than the usual telephone function, and reproducing, and outputting to the exterior.
[0013]Thus, the user of a portable telephone can receive enciphered content data from a distributing server using a portable telephone, and can reproduce the enciphered content data.
[0014]On the other hand, distributing enciphered content data to a personal computer using the Internet is also performed. And in distribution of the enciphered content data to a personal computer, Distribution of enciphered content data is performed by the software installed in the personal computer, and the security to enciphered content data is lower than the case where enciphered content data is written in a memory card. If a personal computer is equipped with a device with the same security as the above-mentioned memory card, it is possible to perform the same distribution as the distribution of enciphered content data to the above-mentioned portable telephone to a personal computer.
[0015]If it does so, a personal computer will receive enciphered content data with the installed software and the above-mentioned device. That is, a personal computer receives the enciphered content data in which security levels differ.
[0016]It is also performed that the audio CD on which music data was recorded has spread widely, and acquires music data from this audio CD by ripping. And the license for decoding encrypted music data (enciphered content data) and its encrypted music data, and reproducing from music data, by this ripping, is generated. And in this ripping, the watermark which makes the use rule of contents data is detected from contents data, and enciphered content data and a license are generated according to the contents of that detected watermark.
[0017]
[Problem(s) to be Solved by the Invention]However, it has only specified that the present watermark generates the license which forbade movement and the duplicate of the license which completely forbid generation of enciphered content data and a license, or decode enciphered content data and are reproduced. Therefore, even if enciphered content data and a license are acquirable by ripping, can move the enciphered content data and license, or they cannot be reproduced. The appearance of the watermark which accepted the use regularity of contents data still more widely is also assumed, and ripping which suited such a watermark cannot be performed by the present ripping from now on.
[0018]then, this invention is made in order to solve this problem, and it comes out. The purpose is to provide the Data Terminal Equipment which can carry out ripping of the contents data according to the use regularity of data.

[0019]
[The means for solving a technical problem and an effect of the invention] The

enciphered content data which the Data Terminal Equipment by this invention acquired the contents data of the plaintext, and enciphered contents data, It is a Data Terminal Equipment which generates the local license for decoding enciphered content data and reproducing, A local license is generated based on the duplicate propriety information included in contents data, The enciphered content creating means which enciphers contents data and generates enciphered content data with the license key contained in the generated local license, A cipher-processing means to generate the encryption local license which gave encryption original with the generated local license, Having a memory measure which memorizes an encryption local license and enciphered content data, and a control section, a control section gives the acquired contents data to an enciphered content creating means, and gives a local license to a cipher-processing means.

[0020]In a Data Terminal Equipment by this invention, duplicate propriety information included in contents data of a plaintext is detected, and a local license is generated according to the contents of that detected duplicate propriety information. A local license contains a license key for enciphering contents data. If a local license is generated, with a license key contained in a local license, contents data will be enciphered and enciphered content data will be generated. And original encryption is given and a generated local license is memorized by memory measure with enciphered content data as an encryption local license.

[0021]Therefore, according to this invention, a local license which decodes enciphered content data and its enciphered content data, and is reproduced according to duplicate propriety information from contents data of a plaintext is generable.

[0022]Enciphered content data in which a Data Terminal Equipment by this invention enciphered contents data, A license for decoding enciphered content data and reproducing is received from a distributing server, And/or, it is a Data Terminal Equipment which generates a local license for acquiring contents data, decoding enciphered content data and enciphered content data, and reproducing, A license management device which performs mutual recognition between distributing servers, and receives enciphered content data and a license from a distributing server, and holds a license, A local license is generated based on duplicate propriety information included in contents data, An enciphered content creating means which enciphers contents data and generates enciphered content data with a license key contained in the generated local license, A cipher-processing means to generate an encryption local license which gave encryption original with a generated local license, Have a memory measure which memorizes a license, an encryption local license, and enciphered content data, and a control section, and a control section gives acquired contents data to an enciphered content creating means, A local license is given to a cipher-processing means.

[0023]While enciphered content data and a license are received from a distributing server and a license is held by hardware in a Data Terminal Equipment by this invention, Enciphered content data and a local license are generated from contents data of a plaintext, original encryption is given and a local license is held by software.

[0024]Therefore, according to this invention, in a Data Terminal Equipment which can receive enciphered content data and a license from a distributing server, enciphered content data and a local license are generable from contents data of a plaintext according to duplicate propriety information.

[0025]Enciphered content data in which a Data Terminal Equipment by this invention enciphered contents data, A license for decoding enciphered content data and reproducing is received from a distributing server, And/or, are a local license for acquiring contents data, decoding enciphered content data and enciphered content data, and reproducing a Data Terminal Equipment to generate, and by software. A license

management module which performs mutual recognition between distributing servers, and receives enciphered content data and a license from a distributing server, A local license is generated based on duplicate propriety information included in contents data, An enciphered content creating means which enciphers contents data and generates said enciphered content data with a license key contained in the generated local license, A cipher-processing means to generate an encryption license which gave encryption original with a received license which gave encryption original with a generated local license, and to which it encryption-local-licensed, Have a memory measure which memorizes an encryption license, an encryption local license, and enciphered content data, and a control section, and a control section, Acquired contents data is given to an enciphered content creating means, and a local license and a license are given to a cipher-processing means.

[0026]While enciphered content data and a license are received from a distributing server and a license is held by software in a Data Terminal Equipment by this invention, Enciphered content data and a local license are generated from contents data of a plaintext, original encryption is given and a local license is held by software.

[0027]Therefore, according to this invention, in a Data Terminal Equipment which can receive enciphered content data and a license from a distributing server, enciphered content data and a local license are generable [from contents data of a plaintext] by software according to duplicate propriety information.

[0028]Enciphered content data in which a Data Terminal Equipment by this invention enciphered contents data, A license for decoding enciphered content data and reproducing is received from a distributing server, And/or, it is a Data Terminal Equipment which generates a local license for acquiring contents data, decoding enciphered content data and enciphered content data, and reproducing, By a license management device which performs mutual recognition between distributing servers, and receives enciphered content data and a license from a distributing server, and holds a license, and software. A license management module which performs mutual recognition between distributing servers, and receives enciphered content data and a license from a distributing server, A local license is generated based on duplicate propriety information included in contents data, An enciphered content creating means which enciphers contents data and generates enciphered content data with a license key contained in the generated local license, and an encryption local license which gave encryption original with a generated local license, Or a cipher-processing means to generate an encryption license which gave encryption original with a license received with a license management module, Having a memory measure which memorizes an encryption license, an encryption local license, and enciphered content data, and a control section, a control section gives acquired contents data to an enciphered content creating means, and gives a license and a local license to a cipher-processing means.

[0029]A Data Terminal Equipment by this invention acquires enciphered content data and a license by three methods. The 1st method is a method of receiving enciphered content data and a license from a distributing server, and holding a license by hardware. The 2nd method is methods of software receiving enciphered content data and a license, and holding a license. And the 3rd method is the methods of generating enciphered content data and a local license from contents data of a plaintext, giving encryption original with a local license, and holding by software.

[0030]Therefore, in [according to this invention] a Data Terminal Equipment which can receive enciphered content data and a license by hardware and software from a distributing server, According to duplicate propriety information, enciphered content data and a local license are generable from contents data of a plaintext.

[0031]Preferably an enciphered content creating means of a Data Terminal Equipment,

Generating further a number for lending out enciphered content data and a local license which were generated to other devices which can be lent out, a cipher-processing means gives encryption original with a local license and a number which can be lent out, and generates an encryption local license.
[0032]When generating enciphered content data and a local license from contents data of a plaintext in a Data Terminal Equipment, A number for lending out enciphered content data and a local license to other devices which can be lent out is generated, and the generated number which can be lent out is enciphered and managed with a local license.
[0033]. Therefore, according to this invention, generate enciphered content data and a local license from contents data of a plaintext. Enciphered content data and a local license which were acquired by what is called ripping can be taken out from a Data Terminal Equipment with which enciphered content data and a local license were held.
[0034]Having further a file generating means to generate preferably a license management file which includes an encryption local license at least, a control section gives enciphered content data and a license management file to a memory measure.
[0035]An encryption local license generated and enciphered in a Data Terminal Equipment is recorded on a license management file, and is held at a memory measure.
[0036]Therefore, in this invention, a generated local license is put into a file and can be managed in soft.
[0037]Preferably, an enciphered content creating means of a Data Terminal Equipment generates a local license reflecting duplicate permit information, when duplicate propriety information is the duplicate permit information to which a duplicate is permitted.
[0038]When duplicate propriety information included in contents data of a plaintext is the duplicate permit information of permitting a duplicate up to 10 times, for example, local licenses including the number of times of duplicate permission which permitted a duplicate up to 10 times are generated.
[0039]Therefore, according to this invention, if contents data can be reproduced, based on duplicate permit information, enciphered content data and a local license which can be reproduced are generable.
[0040]Preferably an enciphered content creating means of a Data Terminal Equipment, When duplicate propriety information is the duplicate permit information to which a duplicate is permitted, a local license reflecting duplicate permit information is generated and contents data does not include duplicate propriety information, A local license which forbade a duplicate and movement of a license for decoding enciphered content data and reproducing is generated.
[0041]When duplicate propriety information included in contents data of a plaintext is what permits a duplicate of contents data, When a local license to which a duplicate of enciphered content data and a local license is permitted according to the contents of permission is generated and contents data does not include duplicate propriety information, A local license which forbids a duplicate and movement of enciphered content data and a license is generated. That is, when contents data is contents data of a kind which does not include duplicate propriety information, a Data Terminal Equipment, A local license which makes it the contents to forbid a duplicate and movement of enciphered content data and a local license which were generated by ripping although a local license is ungenerable according to duplicate propriety information is generated, Enciphered content data and a local license are acquired by ripping.
[0042]Therefore, a local license which determined enciphered content data and the contents of a duplicate of a local license according to a kind of contents data inputted

into a Data Terminal Equipment is generable.
[0043]Preferably, a Data Terminal Equipment is further provided with a medium driving means which drives a recording medium which recorded contents data, and a control section gives contents data which a medium driving means read from a recording medium to an enciphered content creating means.
[0044]If a Data Terminal Equipment is equipped with a recording medium with which contents data was recorded, a medium driving means will read contents data from a recording medium. And a control section gives contents data which a medium driving means read to an enciphered content creating means, and an enciphered content creating means, A local license is generated according to duplicate propriety information included in contents data, with a license key contained in the local license, contents data is enciphered and enciphered content data is generated.
[0045]Therefore, according to this invention, enciphered content data and a local license are acquirable from contents data recorded and distributed to a medium.
[0046]Preferably, a control section of a Data Terminal Equipment gives contents data received by the Internet to an enciphered content creating means.
[0047]A control section of a Data Terminal Equipment gives contents data of a plaintext distributed by the Internet to an enciphered content creating means. And an enciphered content creating means generates a local license according to duplicate propriety information included in contents data, with a license key contained in the local license, enciphers contents data and generates enciphered content data. "Contents data received by the Internet" gives encryption by a public key etc., does not mean contents data which data gave, was performed and was received between distributing servers, and means contents data distributed by the usual Internet.
[0048]Therefore, according to this invention, enciphered content data and a local license are generable from contents data distributed by the Internet which has spread widely.
[0049]Preferably an enciphered content creating means of a Data Terminal Equipment, A duplicate propriety information detection means which detects duplicate propriety information from contents data, A duplicate propriety information judging means which judges detected duplicate propriety information, a license creating means which generates a local license based on a decision result of a duplicate propriety information judging means, and a cryptographer stage which enciphers contents data with a license key are included.
[0050]Contents data inputted into a Data Terminal Equipment is inputted into an enciphered content creating means. And in an enciphered content creating means, duplicate propriety information is detected from contents data by a duplicate propriety information detection means, and the contents of duplicate propriety information are judged by a duplicate propriety information judging means. And a license creating means generates a local license according to a decision result by a duplicate propriety information judging means. That is, if the contents of duplicate propriety information permit a duplicate of contents data, Generate a local license which set up the number of times of a duplicate of a local license, and when the contents of duplicate propriety information are what forbids a duplicate of contents data, If a local license is not generated and duplicate propriety information is not included, a local license which forbade a duplicate and movement of enciphered content data and a local license is generated. With a license key contained in a generated local license, a cryptographer stage enciphers contents data and generates enciphered content data.
[0051]Therefore, according to this invention, a local license is generated according to the contents of duplicate propriety information included in contents data, and enciphered content data and a local license can be acquired by ripping.
[0052]Preferably an enciphered content creating means of a Data Terminal Equipment,

A duplicate propriety information detection means which detects duplicate propriety information from contents data, A duplicate propriety information judging means which judges detected duplicate propriety information, and a duplicate alteration-of-condition means which changes duplicate conditions based on a decision result of a duplicate propriety information judging means, and is written in contents data, An encoding means which codes contents data from a duplicate alteration-of-condition means to a prescribed method, A license creating means which generates a local license based on a decision result of a duplicate propriety information judging means, and a cryptographer stage which enciphers contents data coded by prescribed method with a license key are included.

[0053]Contents data inputted into a Data Terminal Equipment is inputted into an enciphered content creating means. And in an enciphered content creating means, duplicate propriety information is detected from contents data by a duplicate propriety information detection means, and the contents of duplicate propriety information are judged by a duplicate propriety information judging means. And a license creating means generates a local license according to a decision result by a duplicate propriety information judging means. That is, if the contents of duplicate propriety information permit a duplicate of contents data, Generate a local license which set up the number of times of a duplicate of a local license, and when the contents of duplicate propriety information are what forbids a duplicate of contents data, If a local license is not generated and duplicate propriety information is not included, a local license which forbade a duplicate and movement of enciphered content data and a local license is generated. A duplicate alteration-of-condition means changes duplicate conditions according to a decision result of a duplicate propriety information judging means, and rewrites duplicate propriety information included in contents data by the changed duplicate condition. And an encoding means codes contents data in which duplicate propriety information was rewritten to a prescribed method, and with a license key contained in a generated local license, a cryptographer stage enciphers contents data and generates enciphered content data.

[0054]Therefore, according to this invention, contents data can be lawfully reproduced by writing a use rule of contents data in duplicate propriety information in inside.

[0055]Preferably a license creating means of a Data Terminal Equipment, A content identifier which specifies enciphered content data, and a communication identifier which specifies communication when lending out enciphered content data and a license to other devices, A license key and a recorder access condition over a data recorder which records enciphered content data and a local license, A local license which comprises a playback equipment access condition over a data reproduction apparatus which decodes enciphered content data and is reproduced according to a license is generated.

[0056]A license creating means generates a content identifier which constitutes a local license, a communication identifier, a license key, a recorder access condition, and a playback equipment access condition.

[0057]Therefore, according to this invention, a local license for protecting communication to other devices of enciphered content data acquired by ripping and reproduction is generable.

[0058]Preferably a content identifier and a communication identifier, Comprise a fixed area and a management domain following a fixed area, and a license creating means, A local signal which shows that a content identifier or a communication identifier was generated in a Data Terminal Equipment is written in a fixed area, an identification number corresponding to enciphered content data is written in a management domain, and a content identifier and a communication identifier are generated.

[0059]A license creating means to a fixed area of a content identifier and a communication identifier. A local signal which shows that a content identifier and a communication identifier were generated in a Data Terminal Equipment is written in, and each identification number for specifying communication of contents or contents data as a management domain of a content identifier and a communication identifier is written in.
[0060]Therefore, if a fixed area of a content identifier which constitutes a local license according to this invention, and a communication identifier is seen, it turns out easily that that license was generated with a Data Terminal Equipment.
[0061]Preferably, a license creating means of a Data Terminal Equipment generates a communication identifier and a license key by generating of a random number.
[0062]A license creating means generates a random number based on duplicate propriety information, and generates ********** and a license key.
[0063]Therefore, according to this invention, a communication identifier and a license key which are hard to be detected from the exterior are generable.
[0064]Preferably a recorder access condition which constitutes a local license, The number of times showing propriety and the number of times of possible of reproduction of enciphered content data of refreshable, move copy control information which controls movement and a duplicate of enciphered content data and a local license, and protecting level information showing a protecting level of a local license are comprised.
[0065]As an access condition over a data recorder with which enciphered content data and a local license are recorded, The number of times of refreshable of enciphered content data, enciphered content data, move copy control information of a local license, and a protecting level of a local license are generated.
[0066]Therefore, according to this invention, reproduction, movement, and a duplicate of enciphered content data are controllable by the number of times of refreshable, or move copy control information. According to a protecting level, a local license is manageable.
[0067]The number of times of refreshable which constitutes a recorder access condition preferably, The 1st number of times of refreshable that comprises a fixed value showing a reproduction failure of enciphered content data, The 2nd number of times of refreshable that comprises a variation which carries out monotone decreasing whenever it permits reproduction of enciphered content data, Move copy control information which comprises the 3rd number of times of refreshable that permits reproduction of enciphered content data indefinitely, and constitutes a recorder access condition, The 1st control information that forbids movement and a duplicate of enciphered content data and a local license, The 2nd control information that forbids movement of enciphered content data and a local license, and permits a duplicate of enciphered content data and a local license conditionally, The 3rd control information that permits movement and a duplicate of enciphered content data and a local license conditionally, Movement of enciphered content data and a local license is permitted, and the 4th control information that forbids a duplicate of enciphered content data and a local license, and the 5th control information that permits indefinitely movement and a duplicate of enciphered content data and a local license are comprised.
[0068]Therefore, according to this invention, reproduction of enciphered content data, and movement and a duplicate of enciphered content data and a local license are controllable in detail.
[0069]Preferably the 2nd control information on move copy control information, The 3rd control information on move copy control information contains a variation which carries out a monotone increase for every movement and duplicate of enciphered content data and a local license including a variation which carries out monotone

decreasing for every duplicate of enciphered content data and a local license, and expresses the number of times which can be reproduced.
[0070]Therefore, according to this invention, movement and a duplicate of enciphered content data and a license are controllable by a method according to each contents of movement of enciphered content data and a license, and the duplicate.
[0071]The 1st signal with which a playback equipment access condition shows conversion propriety of reproduction speed of enciphered content data preferably, The 2nd signal that shows propriety of edit of enciphered content data, the 3rd signal that shows size of refreshable enciphered content data, the 4th signal that shows the time of the final day of use of enciphered content data, the 5th signal that shows the time of a use opening day of enciphered content data, and an area code are comprised.
[0072]Therefore, according to this invention, reproduction of enciphered content data is controllable in detail.
[0073]Inhibition information which lending information forbids a loan of enciphered content data and a local license preferably, Monotone decreasing is carried out for every loan of enciphered content data and a local license, and loan permit information which carries out a monotone increase for every return of enciphered content data and a local license is comprised.
[0074]Therefore, according to this invention, a loan to enciphered content data acquired by ripping and other devices of a local license is correctly controllable.
[0075]
[Embodiment of the Invention]It explains in detail, referring to drawings for an embodiment of the invention. Identical codes are given to a portion same in the inside of a figure, or considerable, and the explanation is not repeated.
[0076]Drawing 1 is a schematic diagram for explaining notionally the entire configuration of the data distribution system with which the Data Terminal Equipment (personal computer) by this invention acquires enciphered content data.
[0077]Although explained taking the case of the composition of the data distribution system which distributes digital music data to each personal computer via the memory card 110 equipped with digital music data by the user's cellular phone via the portable telephone network, or the Internet below, When distributing the contents data as other works, for example, image data, dynamic image data, etc., this invention can be applied without being limited in such a case, so that it may become clear by the following explanation.
[0078]With reference to drawing 1, the distribution career 20 relays the distribution request (distribution request) from a user obtained through the self portable telephone network to the distributing server 10. The distributing server 10 which manages the music data in which copyright exists, . [whether the memory card 110 with which the portable telephone user's portable telephone 100 accessed in quest of data distribution was equipped has just authentication data, and] Namely, after performing authenticating processing of whether to be a regular memory card and enciphering music data (it is also called contents data below) with a predetermined cipher system to a just memory card, The license containing the license key for decoding enciphered content data as information required for the cellular phone company which is the distribution career 20 for distributing data in order to reproduce such enciphered content data and enciphered content data is given.
[0079]The distribution career 20 distributes enciphered content data and a license via a portable telephone network and the portable telephone 100 to the memory card 110 with which the portable telephone 100 which transmitted the distribution request through the self portable telephone network was equipped.
[0080]In drawing 1, it has the composition that a portable telephone user's portable

telephone 100 is equipped with the removable memory card 110, for example. The memory card 110 receives the enciphered content data received by the portable telephone 100, and after it decodes the encryption performed in the above-mentioned distribution, it gives it to the music reproduction section (not shown) in the portable telephone 100.
[0081]furthermore -- a portable telephone user passes the head telephone 130 grade linked to the portable telephone 100, for example -- such contents data -- "-- reproducing, " carrying out and hearing is possible.
[0082]By having such composition, first, if the memory card 110 is not used, in response to distribution of contents data, it will become difficult composition from the distributing server 10 to play music.
[0083]By and the thing for which the frequency is calculated in the distribution career 20 whenever it distributes the contents data for one music. If the distribution career 20 presupposes that the royalty generated whenever a portable telephone user receives contents data (download) is collected with the phonecall charges of a portable telephone, it will become easy for an owner of a copyright to secure a royalty.
[0084]In drawing 1, the distributing server 10 receives the distribution request from the user of a personal computer who got through the modem 40 and Internet network 30. So then. [whether the distributing server 10 is accessed using the software provided with the license management module for which the personal computer 50 accessed in quest of data distribution has just authentication data, and] Namely, after enciphering music data with a predetermined cipher system to the personal computer which performed authenticating processing of whether to be a regular license management module, and was provided with the just license management module, Such enciphered content data and a license are transmitted via Internet network 30 and the modem 40. The license management module of the personal computer 50 records the received enciphered content data on a hard disk (HDD) etc. as it is, and after enciphering and protecting the received license, it is recorded on HDD.
[0085]It is having the license management device (hardware) provided with the function as the function in connection with the license management of the license management module of the memory card 110 the personal computer 50 being the same, It is a security level higher than the security level recorded on HDD, namely, distribution of the same security level as having received using the portable telephone 100 and the memory card 110 can be received. The distributing server 10 to enciphered content data and a license are received from the distributing server 10 via the modem 40 and Internet network 30. At this time, a license is directly received and recorded in a license management device using the encryption communication way according to a predetermined procedure between the distributing server 10 and a license management module. Enciphered content data is recorded on HDD as it is. This license management device has a high security level compared with the license management module which holds transmission and reception of a license, and the confidentiality of management in hard like the memory card 110, and holds confidentiality by software. The security level which maintains confidentiality by hardwares, such as the memory card 110 or a license management device, in order to distinguish a security level and a license is called the level 2, Suppose that the license which required the security of the level 2 and was distributed is called level 2 license. Suppose that similarly the security level which maintains confidentiality with software like a license management module is called level 1, and the license which required the security level of level 1 and was distributed is called a level 1 license. A license management device and a license management module are explained in detail later.
[0086]In drawing 1, the personal computer 50, The enciphered content data limited to

local use from the music data acquired from the audio CD (Compact Disk) 60 which recorded music data using the license management module, and the license for reproducing enciphered content data are generated. This processing is called ripping and it is equivalent to the act which acquires enciphered content data and a license from an audio CD. On the character, since a security level is by no means high, the license of the local use by ripping shall be treated as a level 1 license, even if ripping is made by what kind of means. The details of ripping are mentioned later.

[0087]The personal computer 50, It is possible to transmit and receive with the memory card 110 which it connected with the portable telephone 100 and was equipped with enciphered content data and a license by the portable telephone 100 with the USB (UniversalSerial Bus) cable 70. However, the treatment changes with security levels of a license. For details, it mentions later.

[0088]In drawing 1, using a license management module, the personal computer 50 can be restricted to the enciphered content data in which a license management module has the level 1 license managed directly, and can be provided with the function to reproduce. Reproduction of enciphered content data with level 2 license will become possible if a personal computer is equipped with the contents playback circuit which has confidentiality by hardware. The detailed explanation about the reproduction in a personal computer is omitted in order to simplify the explanation in this application.

[0089]Therefore, in the data distribution system shown in drawing 1, The personal computer 50 acquires enciphered content data and a license from an audio CD while receiving enciphered content data and a license from the distributing server 10 via the modem 40 and Internet network 30. The memory card 110 with which the portable telephone 100 was equipped, While receiving enciphered content data and a license from the distributing server 10 via a portable telephone network, the enciphered content data and the license which the personal computer 50 acquired from the distributing server 10 or the audio CD 60 are received. The user of the portable telephone 100 becomes possible [acquiring enciphered content data and a license from an audio CD] by passing the personal computer 50.

[0090]The memory card 110 with which the portable telephone 100 was equipped becomes possible [shunting the enciphered content data and the license which were received from the distributing server 10 via the portable telephone network in the personal computer 50].

[0091]Drawing 2 shows the data distribution system at the time of using the reproduction terminal 102 which does not have the function to receive enciphered content data and a license from the distributing server 10 via a portable telephone network. In the data distribution system shown in drawing 2, the memory card 110 with which the reproduction terminal 102 was equipped receives the enciphered content data and the license which the personal computer 50 acquired from the distributing server 10 or the audio CD 60. Thus, when the personal computer 50 acquires enciphered content data and a license, the user of the reproduction terminal 102 without a communication function can also receive enciphered content data.

[0092]In composition as shown in drawing 1 and drawing 2, Being needed on a system, in order to make refreshable the contents data enciphered and distributed at the user side of a cellular phone or a personal computer, Are a method for distributing the encryption key in communication to the 1st, and to the further 2nd. It is the method itself which enciphers contents data to distribute, and is the composition of realizing contents data protection for preventing further the unapproved copy of the contents data distributed to the 3rd in this way.

[0093]In the time of distribution and generating of each reproductive session especially in an embodiment of the invention, The recorder and data reproduction terminal (the

data reproduction terminal which can reproduce contents is also called the portable telephone or personal computer.) in which the attestation and the check function to the movement destination of these contents data were enriched, and un-attesting or a decode key was torn the following -- it is the same -- by preventing the output of the contents data to receive explains the composition which strengthens the copyright protection of contents data.

[0094]Suppose that the processing which transmits contents data to each portable telephone, each personal computer, etc. is called "distribution" from the distributing server 10 in the following explanation.

[0095]In the data distribution system shown in drawing 1 and drawing 2, drawing 3 is a figure explaining the characteristics, such as data for the communication used, and information.

[0096]First, the data distributed from the distributing server 10 is explained. Dc(s) are contents data of music data etc. Encryption which can decode the contents data Dc with the license key Kc is given. Enciphered content data {Dc} Kc to which encryption which can be decoded with the license key Kc was given is distributed to the user of a cellular phone or a personal computer from the distributing server 10 in this form.

[0097]In the following, it shall be shown that the notation {Y} X gave encryption which can be decoded with the decode key X for the data Y.

[0098]From the distributing server 10, additional information Dc-inf as plaintext information, including the copyright about contents data or server access relation, is distributed with enciphered content data. Transaction ID which is the management codes for specifying distribution of the license key from license key Kc and the distributing server 10, etc. as a license is exchanged between the distributing server 10 and the portable telephone 100 or between the distributing server 10 and the personal computer 50. Transaction ID is used also in order to specify the license by distribution, i.e., a license aiming at use on a local. In order to distinguish what is depended on distribution, and the thing of local use, it is transaction ID of local use which starts in "0", and the head of transaction ID presupposes that it is a beginning [from other than "0"] thing transaction ID by distribution. The content ID which is a code for identifying the contents data Dc as a license, . Are generated based on the license terms of purchase AC included the information, including the number of licenses, functional limitation, etc., determined by the specification from the user side. The reproduction control information ACp etc. which are the access control information ACm which is information about the restriction to access of the license in a recorder (a memory card or a license management device), and the control information about the reproduction in a data reproduction terminal exist. The access control information ACm is specifically control information which is in charge of outputting the license or license key from a memory card, a license management module, and a license management device outside, There are limitation information about movement and the duplicate of the number of times (number which outputs a license key for reproduction) of refreshable, and a license, a security level of a license, etc. In order to reproduce the reproduction control information ACp, after a contents playback circuit receives a license key, it is the information which restricts reproduction and a reproduction term, reproduction speed change restrictions, reproduction range specification (partial license), etc. occur.

[0099]Henceforth, suppose that transaction ID and content ID are combined, it is named license ID generically, the license key Kc, license ID, the access control information ACm, and the reproduction control information ACp are combined, and it is named a license generically.

[0100]the reproduction frequency (0:reproduction improper.) which is the control information to which the access control information ACm restricts reproduction

frequency henceforth for simplification having the number of times of 1 - 254:refreshable, and no 255:restrictions, and movement / duplicate flag (0:move duplication prohibition.) which restricts movement and the duplicate of a license 1: Using only movement as good and a dyadic eye [that 2:move duplicate is good], the reproduction control information ACp shall restrict only the reproduction term (UTCtime code) which is the control information which specifies a refreshable term.
[0101]In an embodiment of the invention, for every class of the portable telephone which reproduces a recorder (a memory card or a license management device) and contents data. The prohibition class lists CRL (Class Revocation List) are employed so that distribution of contents data and reproduction can be forbidden. Below, the sign CRL may express the data in prohibition class lists if needed.
[0102]The prohibition class-lists data CRL which listed the portable telephone with which distribution of a license and reproduction are forbidden, the memory card, the license management module on a personal computer, and the class of the license management device is contained in prohibition class-lists pertinent information. All the apparatus and programs which perform the management, accumulation, and reproduction of a license in connection with contents data protection are the target of a listing.
[0103]While the prohibition class-lists data CRL is managed within the distributing server 10, record maintenance of it is carried out also into a memory card or a license management device. Although it is necessary to upgrade such prohibition class lists at any time, and to update data, About change of data, when distributing the license of enciphered content data, a license key, etc. fundamentally, The update date of the prohibition class lists received from the portable telephone or the personal computer (a license management device or a license management module) is judged, When it is judged that it is not updated as compared with the update date of the prohibition class lists CRL to own, the updated prohibition class lists are distributed to a portable telephone or a personal computer. About change of prohibition class lists, it is also possible to generate the difference CRL which is difference data only reflecting a changed part from the distributing server 10 side, and to have composition added to the prohibition class lists CRL in a memory card or a license management device according to this. The update date CRLdate shall be recorded on the prohibition class lists CRL managed within MEMOKADO or a license management device at the time of updating.
[0104]Thus, by carrying out maintenance employment of the prohibition class lists CRL also not only in a distributing server but in the license managing device (the memory card or the license management device) or license management module which records and manages a license, peculiar to a class namely, on the occasion of reproduction, movement, a duplicate, check-out of a license, etc. . The decode key peculiar to the kind of a contents playback circuit (a portable telephone and a reproduction terminal), a license managing device, or license management module was torn. The license key to the license management module which is operating on a contents playback circuit (a portable telephone and a reproduction terminal), a license managing device, or a personal computer, or supply of a license is forbidden. For this reason, in a portable telephone or a personal computer, reproduction of contents data receives a license management device with a memory card or a personal computer, It becomes impossible to acquire a license via a license management module, and it becomes impossible or to receive new contents data.
[0105]Thus, it is in a memory card or a license management device, or the prohibition class lists CRL which a license management module manages have composition which updates data one by one at the time of distribution. Management of the prohibition class lists CRL in a memory card or a license management device, With an upper level, it

records on the Tampa-proof module (Tamper Resistant Module) of the high level which guarantees confidentiality in hard within a memory card or a license management device independently. Alteration prevention treatment is performed at least and management of the prohibition class lists CRL in a license management module is recorded on HDD of a personal computer, etc. by cipher processing. In other words, it is recorded with the Tampa-proof module of the low level the confidentiality was guaranteed to be by software. Therefore, it has composition which cannot alter the prohibition class-lists data CRL from upper levels, such as a file system and an application program. As a result, copyright protection about data can be made firmer.
[0106]Drawing 4 is a figure explaining the characteristics, such as data for the attestation used in the data distribution system shown in drawing 1 and drawing 2, and information.
[0107]The open encryption keys KPpy and KPmw peculiar to a contents playback circuit, a memory card, a license management device, and a license management module are formed, respectively, The open encryption keys KPpy and KPmw can be decoded, respectively with the secret decode key Kmw peculiar to the secret decode key Kpy and a memory card peculiar to a contents playback circuit, a license management device, and a license management module. These public presentation encryption key and a secret decode key have a different value for every kind of a contents playback device, a memory card, a license management device, and license management module. These open encryption keys and secret decode keys are named generically, a class key is called, and the unit which shares a class public presentation encryption key for these open encryption keys, and shares a class secret decode key and a class key for a secret decode key is called a class. A class changes with the kind of a manufacturing company or product, lots at the time of manufacture, etc.
[0108]Cpy is provided as a class certificate of a contents playback circuit (a portable telephone, a reproduction terminal), and Cmw is provided as a memory card, a license management device, and a class certificate of a license management module. These class certificates have different information for every class of a contents playback circuit, a memory card, a license management device, and a license management module. The Tampa-proof module is torn, or the code with a class key was broken, namely, to the class which the secret decode key revealed, it is listed by prohibition class lists and is the prohibition target of license acquisition.
[0109]The class public presentation encryption key and class certificate of these contents playback circuits, Authentication data {KPpy//Cpy} In the form of KPa, the class public presentation encryption key and class certificate of a memory card and a license management device in the form of authentication data {KPmw//Cmw} KPa, The class public presentation encryption key and class certificate of a license management module are recorded [in the form of authentication data {KPmw//Cmw} KPb] on a data reproduction circuit, a memory card, a license management device, and a license management module, respectively at the time of shipment. Although it will explain to details later, when KPaKPb is an open authentication key common to the whole distribution system and the security level of KPa is the level 2, KPb is used when a security level is level 1.
[0110]As a key for managing data processing in the memory card 110, a license management device, and a license management module, The secret decode key Kmcx peculiar to each which can decode the data enciphered with the open encryption key KPmcx set up for every medium called a memory card, a license management device, and a license management module or management software and the open encryption key KPmcx exists. An individual open encryption key and secret decode key are named generically for every memory card of this, an individual key is called, the open

encryption key KPmcx is called an individual public presentation encryption key, and the secret decode key Kmcx is called an individual secret decode key.
[0111]The data transfer between the outside of a memory card, and a memory card, or the data transfer between the outside of a license management device, and a license management device, Or as an encryption key for the maintenance of secret in the data transfer in a license management inter module, the outside of a license management module, Whenever distribution of contents data and reproduction are performed, the common keys Ks1-Ks3 generated in the distributing server 10, the portable telephone 100, the memory card 110, a license management device, and a license management module are used.
[0112]here, the common keys Ks1-Ks3 are a unit of communication of a distributing server, a contents playback circuit, a memory card, a license management device, or a license management inter module, or a unit of access -- "-- it being a peculiar common key by which it is generated in every session", and, Suppose that these common keys Ks1-Ks3 are also called a "session key" to below.
[0113]These session keys Ks1-Ks3 are managed by having a peculiar value for every session with a distributing server, a contents playback circuit, a memory card, a license management device, and a license management module. Specifically, session key Ks1 is generated for every distribution session by a distributing server. Session key Ks2 is generated for every distribution session and reproduction session with a memory card, a license management device, and a license management module, and session key Ks3 is generated for every reproduction session in a contents playback circuit. In each session, the security intensity in a session can be raised by delivering and receiving these session keys, and transmitting a license key etc. in response to the session key generated by other apparatus, after performing encryption by this session key.
[0114]Drawing 5 is a schematic block diagram showing the composition of the distributing server 10 shown in drawing 1 and drawing 2.
[0115]The distributing server 10 is provided with the following.
The information database 304 for holding delivery information which enciphered contents data according to the prescribed method, such as data and content ID.
The charge database 302 for holding the accounting information which followed the access start to contents data for every user of a cellular phone or a personal computer.
The CRL database 306 which manages the prohibition class lists CRL.
The menu database 307 holding the menu of the contents data held at the information database 304, The distribution recording data base 308 holding the log about distribution of transaction ID etc. which specify distribution of contents data, a license key, etc. for every distribution of a license, The data from the information database 304, the charge database 302, the CRL database 306, the menu database 307, and the distribution recording data base 308 is received via bus BS1, The data processing part 310 for performing predetermined processing, and the communication apparatus 350 for performing data transfer between the distribution career 20 and the data processing part 310 via a communications network.

[0116]The data processing part 310 is provided with the following.
The distribution control part 315 for controlling operation of the data processing part 310 according to the data on bus BS1.
The session key generating part 316 for being controlled by the distribution control part 315 and generating session key Ks1 at the time of a distribution session.
The authentication key attaching part 313 holding two kinds of open authentication keys KPa and KPb for decoding authentication data {KPmw//Cmw} KPa or {KPmw//Cmw} KPb for the attestation sent from the memory card, the license management device, and

the license management module.
Authentication data {KPmw//Cmw} KPa or {KPmw//Cmw} KPb for the attestation sent from the memory card, the license management device, and the license management module is received via communication apparatus 350 and bus BS1, The decoding processing section 312 which performs decoding processing with the open authentication key KPa or KPb from the authentication key attaching part 313, Session key Ks1 generated from the session key generating part 316 which generates session key Ks1, and the session key generating part 316 is enciphered using the class public presentation encryption key KPmw obtained by the decoding processing section 312 for every distribution session, The enciphering processing part 318 for outputting to bus BS1, and the decoding processing section 320 which performs decoding processing in response to the data transmitted after being enciphered by session key Ks1 from bus BS1.

[0117]The data processing part 310 is provided with the following.
The license key Kc and the access control information ACm which are given from the distribution control part 315, The enciphering processing part 326 for enciphering with the individual public presentation encryption key KPmcx for every memory card obtained by the decoding processing section 320, license management device, and license management module.
The enciphering processing part 328 for enciphering further and outputting the output of the enciphering processing part 326 to bus BS1 by session key Ks2 to which it is given from the decoding processing section 320.

[0118]The operation in the distribution session of the distributing server 10 will be later explained in detail using a flow chart.
[0119]Drawing 6 is a schematic block diagram for explaining the composition of the personal computer 50 shown in drawing 1 and drawing 2. The personal computer 50 is provided with the following.
Bus BS2 for performing data transfer of each part of the personal computer 50.
The controller (CPU) 510 for controlling the inside of a personal computer and executing various kinds of programs.
Data bus BS2.
The hard disk (HDD) 530 and CD-ROM drive 540 which are the mass recorders for being connected to data bus BS2, recording a program and data, and accumulating, The keyboard 560 for inputting the directions from a user, and the display 570 for giving a user various kinds of information visually.

[0120]The personal computer 50 is provided with the following.
USB interface 550 for controlling transfer of data between the controller 510 and the terminal 580, when communicating enciphered content data and a license to portable telephone 100 grade.
The terminal 580 for connecting USB cable 70.
Serial interface 555 for controlling transfer of data between the controller 510 and the terminal 585, when communicating via the distributing server 10, Internet network 30, and the modem 40.
The terminal 585 for connecting with the modem 40 by a cable.

[0121]In order to receive enciphered content data etc. from the distributing server 10 to the license management device 520 or the license management module 511 via Internet network 40, the controller 510, While controlling transfer of data between the

distributing servers 10, control at the time of acquiring enciphered content data and a license from an audio CD by ripping via CD-ROM drive 540 is performed. The personal computer 50 is provided with the following.
The license management device 520 which manages the license for exchanging various kinds of keys between the distributing servers 10 when performing reception of the enciphered content data from the distributing server 10, and a license, and reproducing the distributed enciphered content data in hard.
The contents managing module 511 which generates the exclusive license which is a program executed by the controller 510, received distribution of the enciphered content data from the distributing server 10, and a level 1 license, and gave encryption original with the received license.

[0122]Since it is what the license management device 520 delivers and receives the data at the time of receiving enciphered content data and a license from the distributing server 10, and manages in hard the license received in hard, The license of the level 2 which requires a high security level can be treated. On the other hand, the license management module 511 performs transfer of the data at the time of receiving enciphered content data and a license from the distributing server 10 in soft using the program executed by the controller 510, Ripping performs the enciphered content data of local use, and generation of a license from an audio CD, Cipher processing etc. are performed and protected against the acquired license, and it accumulates in HDD530, and manages, and only the level 1 license whose security level is lower than the license management device 520 is treated. When a high security level is the level 2, it cannot be overemphasized that a level 1 license can also be treated.
[0123]Thus, the personal computer 50, The license management module 511 and the license management device 520 for receiving enciphered content data and a license via Internet network 30 from the distributing server 10, CD-ROM drive 540 for acquiring enciphered content data and a license from an audio CD by ripping is built in.
[0124]Drawing 7 is a schematic block diagram for explaining the composition of the reproduction terminal 102 shown in drawing 2.
[0125]The reproduction terminal 102 is provided with the following.
Bus BS3 for performing data transfer of each part of the reproduction terminal 102.
The controller 1106 for controlling operation of the reproduction terminal 102 via bus BS3.
The navigational panel 1108 for giving the directions from the outside to the reproduction terminal 102.
The display panel 1110 for giving a user the information outputted from controller 1106 grade as vision information.

[0126]The reproduction terminal 102 is provided with the following.
The removable memory card 110 for memorizing the contents data (music data) from the distributing server 10, and performing decoding processing.
The memory interface 1200 for controlling transfer of the data between the memory card 110 and bus BS3.
USB interface 1112 for controlling the data transfer between bus BS3 and the terminal 1114, when receiving enciphered content data and a license from the personal computer 50.
The terminal 1114 for connecting USB cable 70.

[0127]The reproduction terminal 102 contains the authentication data attaching part 1500 holding authentication data {KPp1//Cp1} KPa enciphered in the state where the

justification can be further attested by decoding class public presentation encryption key KPp1 and class certificate Cp1 with the open authentication key KPa. Here, the class y of the reproduction terminal 102 presupposes that it is y= 1.
[0128]The reproduction terminal 102 is provided with the following.
The Kp1 attaching part 1502 holding Kp1 which is a decode key peculiar to a class.
The decoding processing section 1504 which obtains session key Ks2 which decoded the data which received from bus BS3 by Kp1, and was generated by the memory card 110.

[0129]The reproduction terminal 102 is provided with the following.
The session key generating part 1508 which generates session key Ks3 for enciphering the data which sets and is carried out on bus BS3 between the memory cards 110 in the reproduction session which reproduces the contents data memorized by the memory card 110 with a random number etc.
When receiving the license key Kc and the reproduction control information ACp from the memory card 110 in the reproduction session of enciphered content data, The enciphering processing part 1506 which enciphers session key Ks3 generated by the session key generating part 1508 by session key Ks2 obtained by the decoding processing section 1504, and is outputted to bus BS3.

[0130]The reproduction terminal 102 is provided with the following.
The decoding processing section 1510 which decodes the data on bus BS3 by session key Ks3, and outputs the license key Kc and the reproduction control information ACp.
The decoding processing section 1516 which decodes in response to enciphered content data {Dc} Kc with the license key Kc acquired from the decoding processing section 1510, and outputs contents data from bus BS3.
The music reproduction section 1518 for reproducing contents data in response to the output of the decoding processing section 1516.
The terminal 1530 for outputting the output of DA converter 1519 which changes the output of the music reproduction section 1518 into an analog signal from a digital signal, and DA converter 1519 to external output devices (graphic display abbreviation), such as a head telephone.

[0131]In drawing 7, the field enclosed with a dotted line constitutes the contents playback device 1550 which decodes enciphered content data and reproduces music data.
[0132]On the other hand, the portable telephone 100 shown in drawing 1 has the function to receive distribution of enciphered content data or a license from the distributing server 10 via a portable telephone network. Therefore, the composition of the portable telephone 100 shown in drawing 1, The antenna for receiving the signal by which wireless transfer is carried out with a portable telephone network in the composition shown in drawing 7, The function with which portable telephones, such as a transmission and reception section for changing into a baseband signal in response to the signal from an antenna, or modulating the data from a portable telephone, and giving an antenna, a microphone, a loudspeaker, and voice codec, are originally provided is provided.
[0133]The operation in each session of each component part of the portable telephone 100 and the reproduction terminal 102 will be later explained in detail using a flow chart.
[0134]Drawing 8 is a schematic block diagram for explaining the composition of the memory card 110 shown in drawing 1 and drawing 2.

[0135]As already explained, as the class public presentation encryption key and class secret decode key of a memory card, KPmw and Kmw are provided and the class certificate Cmw of a memory card is formed, but it shall be expressed with the natural number w= 3 in the memory card 110. The natural number x which identifies a memory card shall be expressed with x= 4.
[0136]Therefore, the memory card 110 is provided with the following.
Authentication data {KPm3//Cm3}. Authentication data attaching part 1400 holding KPa
The Kmc attaching part 1402 holding individual secret decode key Kmc4 which is a peculiar decode key set up for every memory card.
The Km attaching part 1421 holding class secret decode key Km3.
The KPmc attaching part 1416 holding open encryption key KPmc4 which can be decoded by individual secret decode key Kmc4.

[0137]Thus, by forming the encryption key of a recorder called a memory card, it becomes possible to perform management of the distributed contents data or the enciphered license key per memory card so that it may become clear in the following explanation.
[0138]The memory card 110 is provided with the following.
The interface 1424 which delivers and receives a signal via the terminal 1426 between the memory interfaces 1200.
Bus BS4 which exchanges a signal between the interfaces 1424.
The decoding processing section 1422 which outputs session key Ks1 which the distributing server 10 generated in the distribution session from the data given to bus BS4 from the interface 1424 from the Km attaching part 1421 in response to the fact that class secret decode key Km3 to contact Pa.
Perform decoding processing by the open authentication key KPa from the data given to bus BS4 in response to the open authentication key KPa from the KPa attaching part 1414, and a decoding result and the obtained class certificate for the controller 1420.
The decoding processing section 1408 which outputs the obtained class public key to the enciphering processing part 1410, and the enciphering processing part 1406 which enciphers the data selectively given by the change-over switch 1446, and is outputted to bus BS4 with the key selectively given by the change-over switch 1442.

[0139]The memory card 110 is provided with the following.
Distribution and the session key generating part 1418 which generates session key Ks2 in each reproductive session.
The enciphering processing part 1410 which enciphers session key Ks2 which the session key generating part 1418 outputted with the class public presentation encryption keys KPpy and KPmw obtained by the decoding processing section 1408, and is sent out to bus BS4.
The decoding processing section 1412 decoded by session key Ks2 obtained from the session key generating part 1418 in response to the data enciphered by session key Ks2 from bus BS4.
The cipher-processing part 1417 which enciphers the license key Kc and the reproduction control information ACp which were read from the memory 1415 in the reproduction session of enciphered content data with the individual public presentation encryption key KPmcx of other memory cards 110 decoded by the decoding processing section 1412 (!=4).

[0140]The decoding processing section 1404 for the memory card 110 to decode the

data on bus BS4 further by individual public presentation encryption key KPmc4 and individual secret decode key Kmc4 of the memory card 110 which make a pair, The prohibition class-lists data CRL updated one by one by data CRL_dat for the renewal of a version of prohibition class lists, Enciphered content data {Dc} Kc and the license (Kc, ACp, ACm, license ID) for reproducing enciphered content data {Dc} Kc, The memory 1415 for storing in response to additional information Data-inf, the regenerated list of enciphered content data, and the license management file for managing a license from bus BS4 is included. The memory 1415 is constituted by semiconductor memory, for example. The memory 1515 comprises the CRL field 1415A, the license area 1415B, and the data area 1415C. The CRL field 1415A is a field for recording the prohibition class lists CRL. The license area 1415B is a field for recording a license. The data area 1415C Pertinent information Dc-inf of the enciphered content data {Dc} Kc and enciphered content data, It is a field for recording the reproduction list file which records the fundamental information for accessing the license management file which records information required in order to manage a license for every enciphered content, and enciphered content data and the license which were recorded on the memory card. And the exterior to direct access is possible for the data area 1415C. The details of a license management file and a reproduction list file are mentioned later.

[0141]The license area 1415B stores a license per record only for a license called an entry, in order to record a license (license key Kc, the reproduction control information ACp, access-restriction-information ACm, license ID). In accessing to a license, it has a license or the composition of it being stored or specifying an entry to record a license on with an entry number.

[0142]Further, the memory card 110 performs data transfer between the exteriors via bus BS4, and contains the controller 1420 for controlling operation of the memory card 110 in response to reproduction information etc. between bus BS4.

[0143]All the composition except the data area 1415C is constituted by the Tampa-proof module field.

[0144]Drawing 9 is a schematic block diagram showing the composition of the license management device 520 built in the personal computer 50. The point that the license management device 520 does not need the field equivalent to the data area 1415C in MEMOKADO 110, Only by differing in that it has the interface 5224 and the terminal 5226 which differ in the function of the interface 1424, and the shape of the terminal 1426, the same composition as the memory card 110 is comprised fundamentally. The authentication data attaching part 5200 of the license management device 520, the Kmc attaching part 5202, the decoding processing section 5204, the cipher-processing part 5206, the decoding processing section 5208, the cipher-processing part 5210, the decoding processing section 5212, the KPa attaching part 5214, the KPmc attaching part 5216, The cipher-processing part 5217, the session key generating part 5218, the controller 5220, the Km attaching part 5221, the decoding processing section 5222, the interface 5224, the terminal 5226, and the change-over switch 5242-5246, Respectively, The authentication data attaching part 1400 of the memory card 110, the Kmc attaching part 1402, the decoding processing section 1404, the cipher-processing part 1406, the decoding processing section 1408, the cipher-processing part 1410, the decoding processing section 1412, the KPa attaching part 1414, the KPmc attaching part 1416, the cipher-processing part 1417, It is the same as the session key generating part 1418, the controller 1420, the Km attaching part 1421, the decoding processing section 1422, and the change-over switch 1442-1446. However, the authentication data attaching part 5200 holds authentication data {KPm7//Cm7} KPa, and the KPmc attaching part 5216, Individual public presentation encryption key KPm8 is held, the Km attaching part 5202 holds class secret decode key Km7, and the Kmc attaching part 5221 holds individual

secret decode key Kmc8. The natural number w showing the class of the license management device 520 is w= 7, and the natural number x for identifying the license management device 520 presupposes that it is it x= 8.
[0145]The memory 5215 which records the prohibition class lists CRL and a license (Kc, ACp, ACm, license ID) is replaced with the memory 1415 of the memory card 110, and the license management device 520 contains it. The memory 5215 comprises the CRL field 5215A which recorded the prohibition class lists CRL, and the license area 5215B which recorded the license.
[0146]Hereafter, operation of each session in the data distribution system shown in drawing 1 and drawing 2 is explained.
[0147][Distribution 1] In the data distribution system shown in drawing 1 and drawing 2, the operation which distributes enciphered content data and a license to the license management device 520 of the personal computer 50 from the distributing server 10 is explained first. This operation is called "distribution 1."
[0148]The distribution operation to the license management device 520 built in the personal computer 50 which generates drawing 10 - drawing 13 at the time of the purchase of the enciphered content data in the data distribution system shown in drawing 1 and drawing 2. They are the 1st for explaining (it is also hereafter called a distribution session) - the 4th flow chart.
[0149]Before the processing in drawing 10, the user of the personal computer 50 connects via the modem 40 to the distributing server 10, and is premised on acquiring the content ID to the contents which wish to purchase.
[0150]With reference to drawing 10, the distribution request by specification of content ID is made via the keyboard 560 from the user of the personal computer 50 (Step S100). And the terms of purchase AC for purchasing the license of enciphered content data via the keyboard 560 are inputted (Step S102). That is, in order to purchase the license key Kc which decodes selected enciphered content data, the access control information ACm of enciphered content data and the reproduction control information ACp are set up, and the terms of purchase AC are inputted.
[0151]If the terms of purchase AC of enciphered content data are inputted, the controller 510 will give the output instruction of authentication data to the license management device 520 via bus BS2 (Step S104). The controller 5220 of the license management device 520 receives the output instruction of authentication data via the terminal 5226, the interface 5224, and bus BS5. And the controller 5220 reads authentication data {KPm7//Cm7} KPa from the authentication data attaching part 5200 via bus BS5, and outputs {KPm7//Cm7} KPa via bus BS5, the interface 5224, and the terminal 5226 (Step S106).
[0152]The controller 510 of the personal computer 50, In addition to authentication data {KPm7//Cm7} KPa from the license management device 520, the data AC and the distribution request of content ID and license terms of purchase are transmitted to the distributing server 10 (Step S108).
[0153]In the distributing server 10, from the personal computer 50 to a distribution request. The data AC of content ID, authentication data {KPm7//Cm7} KPa, and license terms of purchase is received (Step S110), Decoding processing is performed for the authentication data outputted from the license management device 520 in the decoding processing section 312 with the open authentication key KPa (Step S112).
[0154]Authenticating processing which judges whether the distribution control part 315 received the authentication data enciphered for proving the justification in a regular organization from the decoding processing result in the decoding processing section 312 is performed (Step S114). When it is judged that it is just authentication data, the distribution control part 315 recognizes and receives class public presentation

encryption key KPm7 and class certificate Cm7. And it shifts to the next processing (Step S116). In not being just authentication data, it is considered as non approval, and it ends a distribution session without receiving class public presentation encryption key KPm7 and class certificate Cm7 (Step S198).

[0155]When class public presentation encryption key KPm7 and class certificate Cm7 are received as a result of attestation, the distribution control part 315, Next, it refers for whether class certificate Cm7 of the license management device is listed by the prohibition class lists CRL to the CRL database 306, When these class certificates have been the targets of prohibition class lists, a distribution session is ended here (Step S198).

[0156]On the other hand, when the class certificate of the license management device 520 is outside the object of prohibition class lists, it shifts to the next processing (Step S116).

[0157]In [if it is checked that it is access from the personal computer provided with a license management device with just authentication data as a result of attestation, and a class is outside the object of prohibition class lists] the distributing server 10, The distribution control part 315 generates transaction ID which is the management codes for specifying distribution (Step S118). The session key generating part 316 generates session key Ks1 for distribution (Step S120). Session key Ks1 is enciphered by the enciphering processing part 318 by class public presentation encryption key KPm7 corresponding to the license management device 520 obtained by the decoding processing section 312 (Step S122).

[0158]Transaction ID and session key Ks1 which were enciphered are outputted outside via bus BS1 and the communication apparatus 350 as transaction ID//{Ks1} Km7 (Step S124).

[0159]If the personal computer 50 receives transaction ID//{Ks1} Km7 with reference to drawing 11 (Step S126), the controller 510 will input transaction ID//{Ks1} Km7 into the license management device 520 (Step S128). In [if it does so] the license management device 520, The received data given to bus BS5 via the terminal 5226 and the interface 5224, By carrying out decoding processing by class secret decode key Km7 [peculiar to the license management device 520 held at the attaching part 5221], the decoding processing section 5222 decodes session key Ks1, and receives session key Ks1 (Step S130).

[0160]The controller 5220 directs generation of session key Ks2 generated in the license management device 520 to the session key generating part 5218 at the time of distribution operation, if acceptance of session key Ks1 generated with the distributing server 10 is checked. And the session key generating part 5218 generates session key Ks2 (Step S132).

[0161]In a distribution session, the controller 5220 extracts the update date CRLdate from the prohibition class lists CRL currently recorded on the memory 5215 in the license management device 520, and outputs it to the change-over switch 5246 (Step S134).

[0162]The enciphering processing part 5206 by session key Ks1 given from the decoding processing section 5222 via contact Pa of the change-over switch 5242. The update date CRLdate of session key Ks2 given by switching the point of contact of the change-over switch 5246 one by one, individual public presentation encryption key KPmc8, and prohibition class lists is enciphered as one data row, {Ks2//KPmc8//CRLdate} Ks1 is outputted to bus BS3 (Step S136).

[0163]Ks2//KPmc8//encryption data {CRLdate} Ks1 outputted to bus BS3, It is outputted to the personal computer 50 via the interface 5224 and the terminal 5226 from bus BS3, and is transmitted to the distributing server 10 from the personal computer 50

(Step S138).
[0164]The distributing server 10 receives transaction ID//{Ks2//KPmc8//CRLdate} Ks1, In the decoding processing section 320, decoding processing by session key Ks1 is performed, The update date CRLdate of the prohibition class lists CRL in session key Ks2 generated with the license management device 520, open encryption key KPmc8 [peculiar to the license management device 520], and the license management device 520 is received (Step S142).
[0165]The distribution control part 315 generates the access control information ACm and the reproduction control information ACp according to the data AC of the content ID acquired at Step S110, and license terms of purchase (Step S144). The license key Kc for decoding enciphered content data is acquired from the information database 304 (Step S146).
[0166]The distribution control part 315 gives the generated license, i.e., transaction ID, content ID, license key Kc, the reproduction control information ACp, and the access control information ACm to the enciphering processing part 326. The enciphering processing part 326, By open encryption key KPmc8 [peculiar to the license management device 520 obtained by the decoding processing section 320], a license is enciphered and encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc8 is generated (Step S148).
[0167]With reference to drawing 12, the update date CRLdate of the prohibition class lists transmitted from the license management device 520 in the distributing server 10. It is judged whether the prohibition class lists CRL which the license management device 520 holds by being compared with the update date of the prohibition class lists CRL of the distributing server 10 held at the CRL database 306 are the newest, When the prohibition class lists CRL which the license management device 520 holds are judged to be the newest, it shifts to Step S152. When the prohibition class lists CRL which the license management device 520 holds are not the newest, it shifts to Step S160 (Step S150).
[0168]When judged as the newest, the enciphering processing part 328, Encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc8 outputted from the enciphering processing part 326 is enciphered by session key Ks2 generated in the license management device 520, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc8} Ks2 is outputted to bus BS1. And the distribution control part 315 transmits encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc8} Ks2 on bus BS1 to the personal computer 50 via the communication apparatus 350 (Step S152).
[0169]And the controller 510 of the personal computer 50 receives encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc8} Ks2 (Step S154), and inputs it into the license management device 520 via bus BS5. The decoding processing section 5212 of the license management device 520, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc8} Ks2 is received via the terminal 5226 and the interface 5224, It decodes by session key Ks2 generated by the session key generating part 5218, and {transaction ID// content ID//Kc//ACm//ACp} Kmc8 is received (Step S158). Then, it shifts to Step S172.
[0170]When the prohibition class lists CRL which the license management device 520 holds are judged not to be the newest, on the other hand in the distributing server 10, the distribution control part 315, The newest prohibition class lists CRL are acquired from the CRL database 306 via bus BS1, and the difference CRL which is difference data is generated (Step S160).
[0171]The enciphering processing part 328 is enciphered by session key Ks2 generated in the license management device 520 in response to the output of the enciphering

processing part 326, and the difference CRL of the prohibition class lists which the distribution control part 315 supplies via bus BS1. Difference CRL/encryption data {/{transaction ID// content ID//Kc//ACm//ACp} Kmc8} Ks2 outputted from the enciphering processing part 328 is transmitted to the personal computer 50 via bus BS1 and the communication apparatus 350 (Step S162).

[0172]The personal computer 50 receives difference CRL/encryption data {/{transaction ID// content ID//Kc//ACm//ACp} Kmc8} Ks2 transmitted (Step S164), It inputs into the license management device 520 via bus BS5 (Step S166). In the license management device 520, the received data given to bus BS5 are decoded by the decoding processing section 5212 via the terminal 5226 and the interface 5224. The decoding processing section 5212 decodes the received data of bus BS5 using session key Ks2 given from the session key generating part 5218, and outputs them to bus BS5 (Step S168).

[0173]In this stage, encryption license {transaction ID// content ID//Kc//ACm//ACp} Kmc8} which can be decoded by secret decode key Kmc8 held at the Kmc attaching part 5221, and the difference CRL are outputted to bus BS5 (Step S168). The CRL field 5215A in the memory 5215 is updated based on the difference CRL by the difference CRL received with directions of the controller 5220 (Step S170).

[0174]Step S152, S154, S156, and S158, It is distribution operation to the license management device 520 of a license in case the prohibition class lists CRL of the license management device 520 are the newest, Step S160, S162, S164, S166, S168, and S170 are distribution operations to the license management device 520 of a license in case the prohibition class lists CRL of the license management device 520 are not the newest. By thus, the update date CRLdate of the prohibition class lists sent from the license management device 520. When it checks in detail whether the prohibition class lists CRL of the license management device 520 which has asked for distribution are the newest and is not the newest, Distribution of the license to the license management device with which the license was broken can be prevented by acquiring the newest prohibition class lists CRL from the CRL database 306, and distributing the difference CRL to the license management device 520.

[0175]With directions of the controller 5220 after Step S158 or Step S170. Encryption license {transaction ID// content ID//Kc//ACm//ACp} Kmc8, In the decoding processing section 5204, it is decoded by individual secret decode key Kmc8, and a license (license key Kc, transaction ID, content ID, the access control information ACm, and reproduction control information ACp) is received (Step S172).

[0176]With reference to drawing 13, the controller 510 inputs into the license management device 520 the entry number for directing the entry which stores the license which the license management device 520 received (Step S174). So then, the controller 5220 of the license management device 520, An entry number is received via the terminal 5226 and the interface 5224, To the license area 5215B of the memory 5215 specified with the received entry number. The license (license key Kc, transaction ID, content ID, the access control information ACm, and reproduction control information ACp) acquired in Step S172 is stored (Step S176).

[0177]The controller 510 of the personal computer 50 transmits transaction ID sent from the distributing server 10, and the distribution request of enciphered content data to the distributing server 10 (Step S178).

[0178]The distributing server 10 receives the distribution request of transaction ID and enciphered content data (Step S180), From the information database 304, enciphered content data {Dc} Kc and additional information Dc-inf are acquired, and these data is outputted via bus BS1 and the communication apparatus 350 (Step S182).

[0179]The personal computer 50 receives {Dc} Kc//Dc-inf, and receives enciphered

content data {Dc} Kc and additional information Dc-inf (Step S184). If it does so, the controller 510 will record enciphered content data {Dc} Kc and additional information Dc-inf on the hard disk (HDD) 530 via bus BS2 as one contents file (Step S186). The entry number of the license with which the controller 510 was stored in the license management device 520, The license management file to enciphered content data {Dc} Kc and additional information Dc-inf containing transaction ID and content ID of a plaintext is generated, and it records on HDD530 via bus BS2 (Step S188). The controller 510 as information on the contents received to the contents list file currently recorded on HDD530, The name of the recorded contents file and a license management file, The information (a track name, an artist name) about the enciphered content data extracted from additional information Dc-inf, etc. are added (Step S190), and transaction ID and distribution acceptance are transmitted to the distributing server 10 (Step S192).

[0180]If transaction ID// distribution acceptance is received (Step S194), the distributing server 10, Record to storing of the billing data to the charge database 302 and the distribution recording data base 308 of transaction ID is performed, processing of the end of distribution is performed (Step S196), and the whole processing is completed (Step S198).

[0181]Thus, the license management device 50 built in the personal computer 50 is apparatus holding regular authentication data, After checking that open encryption key KPm7 which has enciphered and transmitted with class certificate Cm7 is effective simultaneously, Class certificate Cm7 can distribute contents data only to the distribution request from the license management device which is not written in prohibition class lists, i.e., the class certificate list in which encryption by open encryption key KPm7 was broken, The distribution using the class key to the inaccurate license management device distributed and decoded can be forbidden.

[0182]By exchanging the encryption key generated by the distributing server and a license management module, respectively, performing encryption using the encryption key which each received, and transmitting the encryption data to the other party, De facto mutual recognition can be performed also in transmission and reception of each encryption data, and the security of a data distribution system can be raised.

[0183]When the license management device 520 receives enciphered content data and a license from the distributing server 10, Since the license for exchanging data in hard between the distributing servers 10, and reproducing enciphered content data is stored in hard, the security level is high. Therefore, if the license management device 520 is used, while the personal computer 50 can receive enciphered content data and a license by high distribution of a security level, management of the level 2 license with a high security level is possible for it.

[0184]It is also possible to distribute enciphered content data and a license to the memory card 110 with which the portable telephone 100 shown in drawing 1 was equipped according to the flow chart shown in drawing 10 - 13 via a portable telephone network. Namely, what is necessary is to replace the personal computer 50 with the portable telephone 100, and just to replace the license management device 520 with the memory card 110 in the above-mentioned explanation. In this case, in Step S186 shown in drawing 13, S188, and S190, A contents file (enciphered content data {Dc} Kc and additional information Dc-inf), a license management file, and the reproduction list file replaced with a contents list file are recorded on the data area 1415C of the memory 1415 of the memory card 110. Others are the same as having mentioned above.

[0185]Since it receives in hard and enciphered content data and a license are stored also in the enciphered content data to the memory card 110, and distribution of a license, Management of the level 2 license with a high security level is possible for the

enciphered content data to the memory card 110, and distribution of a license like the enciphered content data to the license management device 520, and distribution of a license.

[0186][Distribution 2] Next, in the data distribution system shown in drawing 1 and drawing 2, the operation which distributes enciphered content data and a license to the license management module 511 of the personal computer 50 from the distributing server 10 is explained. This operation is called "distribution 2."

[0187]Before the processing in drawing 14, the user of the personal computer 50 connects via the modem 40 to the distributing server 10, and is premised on acquiring the content ID to the contents which wish to purchase.

[0188]Drawing 14 - drawing 17 are the 1st for explaining the distribution operation to the license management module 511 built in the personal computer 50 by which it is generated at the time of the purchase of the enciphered content data in the data distribution system shown in drawing 1 and drawing 2 - the 4th flow chart. The license management module 511 performs reception from enciphered content data and the distributing server 10 of a license by a program. Although it is the same as that of "the distribution 1" about the form of the data exchanged with the channel (between the distributing server 10 and the personal computer 50) in "the distribution 2", and the composition of security, the two open authentication keys KPa and KPb are used for a distributing server. KPa is an open authentication key which checks the authentication data of MEMOKADO 110 whose security level is the level 2, and the license management device 520, and KPb is an open authentication key which checks the authentication data of the license management module 511 whose security level is level 1. The license management module 511 is a software module with the almost same composition as the license management device 520. The natural number w showing the class of the license management module 511 is w= 5, and the natural number x for identifying the license management module 511 presupposes that it is it x= 6. Therefore, the license management module 511 holds authentication data {KPm5//Cm5} KPb and individual public presentation encryption key KPm6, class secret decode key Km5, and individual secret decode key Kmc6.

[0189]With reference to drawing 14, the distribution request by specification of content ID is made via the keyboard 560 from the user of the personal computer 50 (Step S200). And the terms of purchase AC for purchasing the license of enciphered content data via the keyboard 560 are inputted (Step S202). That is, in order to purchase the license key Kc which decodes selected enciphered content data, the access control information ACm of enciphered content data and the reproduction control information ACp are set up, and the terms of purchase AC are inputted.

[0190]When the terms of purchase AC of enciphered content data are inputted, the controller 510, Authentication data {KPm5//Cm5} from the license management module 511 KPb is read, The read authentication data {KPm5//Cm5} In addition to KPb, the data AC and the distribution request of content ID and license terms of purchase are transmitted to the distributing server 10 (Step S204).

[0191]In the distributing server 10, the data AC of a distribution request, content ID, authentication data {KPm5//Cm5} KPb, and license terms of purchase is received from the personal computer 50 (Step S206). And the distribution control part 315 distinguishes whether it is requiring whether to demand distribution of level 1 based on class certificate Cm5 of authentication data {KPm5//Cm5} KPb for distribution of the level 2. Authentication data {KPm5//Cm5} Since KPb is authentication data from the license management module 511 which requires distribution of level 1, it recognizes that the distribution control part 315 is a distribution request of level 1. Received authentication data {KPm5//Cm5} KPb is decoded with the level 1-oriented open

authentication key KPb in the decoding processing section 312 (Step S208).
[0192]The distribution control part 315 the distribution control part 315 from the decoding processing result in the decoding processing section 312. Authentication data {KPm5//Cm5} Authenticating processing which judges whether the authentication data which gave the code for KPb to prove the justification in an organization regular as level 1 correspondence was received is performed (Step S210). When it is judged that it is just level 1 authentication data, the distribution control part 315 recognizes and receives open encryption key KPm5 and certificate Cm5. And it shifts to Step S212. When it is judged that the distribution control part 315 is not just authentication data for level 1, it is considered as non approval, and processing is ended without receiving open encryption key KPm5 and certificate Cm5 (Step S288).
[0193]Here, as for the distributing server 10, although explanation is not given in details any more, it is also possible for a security level to transmit a level 1 license to the license management device 520 which is the level 2, or the memory card 110 directly via the personal computer 50.
[0194]When open encryption key KPm5 and certificate Cm5 are received as a result of attestation, the distribution control part 315, Next, it refers for whether class certificate Cm5 of the license management module 511 is listed by the prohibition class lists CRL to the CRL database 306, When these class certificates have been the targets of prohibition class lists, a distribution session is ended here (Step S288).
[0195]On the other hand, when the class certificate of the license management module 511 is outside the object of prohibition class lists, it shifts to the next processing (Step S214).
[0196]In [if open encryption key KPm5 and certificate Cm5 are received and it is checked as a result of attestation that a class certificate is outside the object of prohibition class lists] the distributing server 10, The distribution control part 315 generates transaction ID which is the management codes for specifying distribution (Step S214). The session key generating part 316 generates session key Ks1 for distribution (Step S216). Session key Ks1 is enciphered by the enciphering processing part 318 by class public presentation encryption key KPm5 corresponding to the license management module 511 obtained by the decoding processing section 312 (Step S218).
[0197]Transaction ID and session key Ks1 which were enciphered are outputted outside via bus BS1 and the communication apparatus 350 as transaction ID//{Ks1} Km5 (Step S220).
[0198]With reference to drawing 15, the controller 510 of the personal computer 50, When transaction ID//{Ks1} Km5 are received (Step S222), the license management module 511, In response to the fact that {Ks1} Km5, by class secret decode key Km5 [peculiar to the license management module 511], decoding processing is performed and session key Ks1 is received (Step S224).
[0199]The license management module 511 will generate session key Ks2, if acceptance of session key Ks1 generated with the distributing server 10 is checked (Step S226). And the controller 510 reads the encryption CRL memorized by HDD530 via bus BS2, and the license management module 511, The update date CRLdate of the prohibition class lists CRL to the prohibition class lists which decoded the encryption CRL, and acquired and decoded the prohibition class lists CRL is acquired (Step S228). Further the license management module 511 by session key Ks1 generated in the distributing server 10. The update date CRLdate of session key Ks2 which made it generate by the license management module 511, individual public presentation encryption key KPmc6, and prohibition class lists is enciphered as one data row, and {Ks2//KPmc6//CRLdate} Ks1 is outputted (Step S230).
[0200]The controller 510 transmits transaction ID//{Ks2//KPmc6//CRLdate} Ks1 which

added transaction ID to Ks2//KPmc6//encryption data {CRLdate} Ks1 to the distributing server 10 (Step S232).
[0201]The distributing server 10 receives transaction ID//{Ks2//KPmc6//CRLdate} Ks1 (Step S234), In the decoding processing section 320, decoding processing by session key Ks1 is performed, The update date CRLdate of the prohibition class lists in session key Ks2 generated by the license management module 511, individual public presentation encryption key KPmc6 [peculiar to the license management module 511], and the license management module 511 is received (Step S236).
[0202]The distribution control part 315 generates the access control information ACm and the reproduction control information ACp according to the data AC of the content ID acquired at Step S206, and license terms of purchase (Step S238). The license key Kc for decoding enciphered content data {Dc} Kc is acquired from the information database 304 (Step S240).
[0203]The distribution control part 315 gives the generated license, i.e., transaction ID, content ID, license key Kc, the reproduction control information ACp, and the access control information ACm to the enciphering processing part 326. The enciphering processing part 326, By open encryption key KPmc6 [peculiar to the license management module 511 obtained by the decoding processing section 320], a license is enciphered and encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc6 is generated (Step S242).
[0204]With reference to drawing 16, the update date CRLdate of the prohibition class lists transmitted from the license management module 511 in the distributing server 10. It is judged whether the prohibition class lists CRL which the license management module 511 holds by comparing with the update date of the prohibition class lists CRL of the distributing server 10 held at the CRL database 306 are the newest, When the prohibition class lists CRL which the license management module 511 holds are judged to be the newest, it shifts to Step S246. When the prohibition class lists CRL which the license management module 511 holds are not the newest, it shifts to Step S252 (Step S244).
[0205]When judged as the newest, the enciphering processing part 328, Encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc6 outputted from the enciphering processing part 326 is enciphered by session key Ks2 generated in the license management module 511, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc6} Ks2 is outputted to bus BS1. And the distribution control part 315 transmits encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc6} Ks2 on bus BS1 to the personal computer 50 via the communication apparatus 350 (Step S246).
[0206]And the controller 510 of the personal computer 50, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc6} Ks2 is received (Step S248), The license management module 511 decodes encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc6} Ks2 by session key Ks2, {Transaction ID// content ID//Kc//ACm//ACp} Kmc6 is received (Step S250). Then, it shifts to Step S162.
[0207]When the prohibition class lists CRL which the license management module 511 holds are judged not to be the newest, on the other hand in the distributing server 10, the distribution control part 315, The newest prohibition class lists CRL are acquired from the CRL database 306 via bus BS1, and the difference CRL which is difference data is generated (Step S252).
[0208]The enciphering processing part 328 is enciphered by session key Ks2 generated in the license management module 511 in response to the output of the enciphering processing part 326, and the difference CRL of the prohibition class lists which the distribution control part 315 supplies via bus BS1. Difference CRL/encryption data

{/{transaction ID// content ID//Kc//ACm//ACp} Kmc6} Ks2 outputted from the enciphering processing part 328 is transmitted to the personal computer 50 via bus BS1 and the communication apparatus 350 (Step S254).
[0209]The personal computer 50 receives difference CRL/encryption data {/{transaction ID// content ID//Kc//ACm//ACp} Kmc6} Ks2 transmitted (Step S256), The license management module 511 decodes received data using session key Ks2, and receives the difference CRL and encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc6 (Step S258).
[0210]The controller 510 adds the difference CRL received to the prohibition class lists CRL recorded on HDD530, performs original cipher processing, and rewrites the prohibition class lists CRL in HDD530 (Step S260).
[0211]Step S246, S248, and S250 are distribution operations to the license management modules 511, such as the license key Kc in case the prohibition class lists CRL of the license management module 511 are the newest, Step S252, S254, S256, S258, and S260 are distribution operations to the license management modules 511, such as the license key Kc in case the prohibition class lists CRL of the license management module 511 are not the newest. Thus, when checking in detail and not updating whether the prohibition class lists CRLdate sent from the license management module 511 are updated, Distribution of enciphered content data {Dc} Kc to the license management module in which the license was broken can be prevented by acquiring the newest prohibition class lists CRLdate from the CRL database 306, and distributing the difference CRL to the license management module 511.
[0212]Encryption license {transaction ID// content ID//Kc//ACm//ACp} Kmc6 after Step S250 or Step S260, It is decoded by secret decode key Kmc6 and a license (license key Kc, transaction ID, content ID, the access control information ACm, and reproduction control information ACp) is received (Step S262).
[0213]With reference to drawing 17, the license management module 511 generates the check-out information containing the number for lending out the enciphered content data and the license which were received from the distributing server 10 to other devices which can be checked out (Step S264). In this case, the initial value of check-out is set as "3." So then, the license management module 511, The encryption level 1 extension license which performed cipher processing original with the received license (transaction ID, content ID, license key Kc, the access control information ACm, and reproduction control information ACp) and the generated check-out information is generated (Step S266). In this case, the license management module 511 enciphers based on the identification number of the controller (CPU) 510 of the personal computer 50, etc. Therefore, if the encryption level extension 1 generated license turns into a license original with the personal computer 50 and does not use the check-out mentioned later, it cannot communicate enciphered content data and a license to other devices. Since a security hole exists clearly, movement of a license of an in [management of level 1] in a security level is because movement of the license is not allowed.
[0214]The controller 510 of the personal computer 50 transmits transaction ID sent from the distributing server 10, and the distribution request of enciphered content data to the distributing server 10 (Step S268).
[0215]The distributing server 10 receives the distribution request of transaction ID and enciphered content data (Step S270), From the information database 304, enciphered content data {Dc} Kc and additional information Dc-inf are acquired, and these data is outputted via bus BS1 and the communication apparatus 350 (Step S272).
[0216]The personal computer 50 receives {Dc} Kc//Dc-inf, and receives enciphered content data {Dc} Kc and additional information Dc-inf (Step S274). If it does so, the

controller 510 will record enciphered content data {Dc} Kc and additional information Dc-inf on the hard disk (HDD) 530 via bus BS2 as one contents file (Step S276). The encryption level 1 extension license by which the controller 510 was generated with the license management module 511, The license management file to enciphered content data {Dc} Kc and additional information Dc-inf containing transaction ID and content ID of a plaintext is generated, and it records on HDD530 via bus BS2 (Step S278). The controller 510 as information on the contents received to the contents list file currently recorded on HDD530, The name of the recorded contents file and a license management file, The information (a track name, an artist name) about the enciphered content data extracted from additional information Dc-inf is added (Step S280), and transaction ID and distribution acceptance are transmitted to the distributing server 10 (Step S282).
[0217]If transaction ID// distribution acceptance is received (Step S284), the distributing server 10, Record to storing of the billing data to the charge database 302 and the distribution recording data base 308 of transaction ID is performed, processing of the end of distribution is performed (Step S286), and the whole processing is completed (Step S288).
[0218]Thus, by exchanging the encryption key generated by the distributing server and a license management module, respectively, performing encryption using the encryption key which each received, and transmitting the encryption data to the other party, De facto mutual recognition can be performed also in transmission and reception of each encryption data, and the security of a data distribution system can be raised, And it is the same as that of the case where a license is directly distributed to the license management device 520 and the memory card 110 in the point of employing the prohibition class lists CRL.
[0219]However, in the personal computer 50 the license management module 511, Exchange data by software, receive a license from the distributing server 10, and distribution of the license by the license management module 511 in the point to manage, A security level is lower than distributing a license to the license management device 520 and the memory card 110 directly.
[0220][Movement] In the data distribution system shown in drawing 1 and drawing 2, The operation which transmits the enciphered content data and the license which were distributed to the license management device 520 of the personal computer 50 from the distributing server 10 to the memory card 110 equipped by the portable telephone 100 or the reproduction terminal 102 is explained. This operation is called "movement" and a security level is the processing performed only between the levels 2.
[0221]In the data distribution system which shows drawing 1 and drawing 2 drawing 18 - drawing 21, They are the 1st for explaining the moving operation by which the license management device 520 moves the enciphered content data and the license which were received from the distributing server 10 to the memory card 110 equipped by the portable telephone 100 or the reproduction terminal 102 - the 4th flow chart. In movement, since the portable telephone 100 or the reproduction terminal 102 is apparatus of only relaying data, it has been omitted from the flow chart. In explaining movement, explain the case where it moves to the memory card 110 with which the reproduction terminal 102 of drawing 2 was equipped, but. The same may be said of the case where it moves to the memory card 110 with which the portable telephone 100 of drawing 1 was equipped, and reading ****** is good for the portable telephone 100 in the reproduction terminal 102.
[0222]Before the processing in drawing 18, the user of the personal computer 50 determines the contents which move according to a contents list file, and explains as a premise that the contents file and the license management file can be specified.
[0223]When a move request is inputted from the keyboard 560 of the personal computer

50 with reference to drawing 18 (Step S300), the controller 510, The Request to Send of authentication data is transmitted to the reproduction terminal 102 via USB interface 550, the terminal 580, and USB cable 70 (Step S302). So then, the controller 1106 of the reproduction terminal 102, The Request to Send of authentication data is received via terminal 1114, USB interface 1112, and bus BS3, and the Request to Send of authentication data is transmitted to the memory card 110 via bus BS3 and the memory card interface 1200. And the controller 1420 of the memory card 110 receives the Request to Send of authentication data via the terminal 1426, the interface 1424, and bus BS4 (Step S304).

[0224]The controller 1420 will read authentication data {KPm3//Cm3} KPa from the authentication data attaching part 1400 via bus BS4, if the Request to Send of authentication data is received, The read authentication data {KPm3//Cm3} KPa is outputted to the reproduction terminal 102 via bus BS4, the interface 1424, and the terminal 1426. And the controller 1106 of the reproduction terminal 102, Authentication data {KPm3//Cm3} KPa is received via the memory card interface 1200 and bus BS3, Authentication data {KPm3//Cm3} KPa is transmitted to the personal computer 50 via bus BS3, USB interface 1112, the terminal 1114, and USB cable 70 (Step S306).

[0225]So then, the controller 510 of the personal computer 50, Authentication data {KPm3//Cm3} KPa is received via the terminal 580 and USB interface 550 (Step S308), and the authentication data {KPm3//Cm3} KPa which received is transmitted to the license management device 520 via bus BS2. The controller 5220 of the license management device 520 receives authentication data {KPm3//Cm3} KPa via the terminal 5226, the interface 5224, and bus BS5, and gives the authentication data {KPm3//Cm3} KPa which received to the decoding processing section 5208. The authentication processing part 5208 performs decoding processing of authentication data {KPm3//Cm3} KPa with the authentication key KPa from the KPa attaching part 5214 (Step S310). The controller 5220 from the decoding processing result in the decoding processing section 5208. In order that whether processing having been performed normally and the memory card 110 may attest holding class public presentation encryption key KPm3 from a regular memory card, and class certificate Cm3, Authenticating processing which judges whether the authentication data which gave the code for proving the justification in a regular organization was received is performed (Step S312). When it is judged that it is just authentication data, the controller 5220 recognizes and receives class public presentation encryption key KPm3 and class certificate Cm3. And it shifts to the next processing (Step S314). In not being just authentication data, it is considered as non approval, and it ends processing without receiving class public presentation encryption key KPm3 and class certificate Cm3 (Step S404).

[0226]In order that the license management device 520 may hold only the open authentication key KPa of level 2 correspondence here, Since attestation goes wrong and processing is temporarily ended when a security level is the demand from the license management module 511 which is level 1, movement to level 1 from the level 2 cannot be performed.

[0227]When it is recognized as a result of attestation that it is a regular memory card, the controller 5220, Next, it refers for whether class certificate Cm3 of the memory card 110 is listed by the prohibition class lists CRL to the CRL field 5215A of the memory 5215, When these class certificates have been the targets of prohibition class lists, moving operation is ended here (Step S404).

[0228]On the other hand, when the class certificate of the memory card 110 is outside the object of prohibition class lists, it shifts to the next processing (Step S314).

[0229]In [if it is checked that it is access from the reproduction terminal provided with

a memory card with just authentication data as a result of attestation, and a class is outside the object of prohibition class lists] the license management device 520, The controller 5220 acquires transaction ID which is management codes from the license area 5215B of the memory 5215 (Step S316). And the session key generating part 5218 generates session key Ks22 for movement (Step S318). Session key Ks22 is enciphered by the enciphering processing part 5210 by class public presentation encryption key KPm3 corresponding to the memory card 110 obtained by the decoding processing section 5208 (Step S320). The controller 5220 acquires encryption data {Ks22} Km3 via bus BS5, Transaction ID//{Ks22} Km3 which added transaction ID acquired from the memory 5215 to encryption data {Ks22} Km3 are outputted via bus BS5, the interface 5224, and the terminal 5226 (Step S322).

[0230]With reference to drawing 19, the controller 510 of the personal computer 50, Transaction ID//{Ks22} Km3 are received via bus BS2 (Step S324), Transaction ID//{Ks22} Km3 are transmitted to the reproduction terminal 102 via USB interface 550, the terminal 580, and USB cable 70 (Step S324). So then, the controller 1106 of the reproduction terminal 102, Transaction ID//{Ks22} Km3 are received via terminal 1114, USB interface 1112, and bus BS3, and its transaction ID// {Ks22} Km3 which received are transmitted to the memory card 110 via the memory card interface 1200. And the controller 1420 of the memory card 110 receives transaction ID//{Ks22} Km3 via the terminal 1426, the interface 1424, and bus BS4 (Step S326). The decoding processing section 1422 receives {Ks22} Km3 from the controller 1420 via bus BS4, by class secret decode key Km3 from the Km attaching part 1421, decodes {Ks22} Km3 and receives session key Ks22 (Step S328). And the session key generating part 1418 generates session key Ks2 (Step S330), and the controller 1420, The update date CRLdate of prohibition class lists is acquired from the CRL field 1415A of the memory 1415 via bus BS4, and the acquired update date CRLdate is given to the change-over switch 1446 (Step S332).

[0231]So then, the update date CRLdate of session key Ks2 acquired when the enciphering processing part 1406 switched the terminal of the change-over switch 1446 one by one, individual public presentation encryption key KPmc4, and prohibition class lists. It enciphers by session key Ks22 decoded by the decoding processing section 1404, and Ks2//KPmc4//encryption data {CRLdate} Ks22 are generated. The controller 1420 outputs Ks2//KPmc4//encryption data {CRLdate} Ks22 to the reproduction terminal 102 via bus BS4, the interface 1424, and the terminal 1426, The controller 1106 of the reproduction terminal 102 receives Ks2//KPmc4//encryption data {CRLdate} Ks22 via the memory card interface 1200. And the controller 1106 transmits to the personal computer 50 via USB interface 1112, the terminal 1114, and USB cable 70 (Step S334).

[0232]The controller 510 of the personal computer 50, Ks2//KPmc4//encryption data {CRLdate} Ks22 are received via the terminal 580 and USB interface 550 (Step S336), Ks2//KPmc4//encryption data {CRLdate} Ks22 are inputted into the license management device 520 via bus BS2 (Step S338). The controller 5220 of the license management device 520, Ks2//KPmc4//encryption data {CRLdate} Ks22 are received via the terminal 5226, the interface 5224, and bus BS5, and its Ks2//KPmc4// encryption data {CRLdate} Ks22 which received are given to the decoding processing section 5212. The decoding processing section 5212 decodes Ks2//KPmc4//encryption data {CRLdate} Ks22 by session key Ks22 from the session key generating part 5218, The update date CRLdate of session key Ks2, open encryption key KPmc4, and prohibition class lists is received (Step S340).

[0233]If it does so, the controller 510 of the personal computer 50 will read the entry number of the license included in the license management file recorded on HDD530 in Step S324 from HDD530. And the controller 510 inputs the read entry number into the

license management device 520 via bus BS2 (Step S342). The controller 5220 of the license management device 520, An entry number is received via the terminal 5226, the interface 5224, and bus BS5, A license (transaction ID, content ID, license key Kc, access-control-information ACm, reproduction control information ACp) is read from the entry of the license area 5215B of the memory 5215 specified with an entry number (Step S344).

[0234]The controller 5220 ranks second and checks the access control information ACm (Step S346). That is, based on the access control information ACm which acquired the controller 5220, It is checked whether the license which first is going to move to the memory card 110 with which the reproduction terminal 102 was equipped is the license which cannot perform reproduction of enciphered content data by reproduction frequency. It is because there is no meaning which moves to the memory card 110 which could not reproduce enciphered content data according to a license, but was equipped with the enciphered content data and license by the reproduction terminal 102 when reproduction frequency does not remain (reproduction frequency =0). When it cannot reproduce and can reproduce, the duplicate of a license and the propriety of movement are judged with movement / duplicate flags.

[0235]In Step S346, reproduction frequency of enciphered content data is not made (reproduction frequency =0), or when movement / duplicate flags are move duplication prohibition (=0), by the access control information ACm, it judges that duplicate movement is impossible, and shifts to Step S404, and moving operation is ended. Reproduction of enciphered content data can be performed in Step S346 (reproduction frequency !=0), And movement / duplicate flags are judged that only movement is movement of a license in the case of C "=1", and the controller 510 deletes the license in the entry number specified in the license area 5215B of the memory 5215 (Step S348), and shifts to Step S350. Reproduction of enciphered content data can be performed, and when "reproduction frequency !=0" and movement / duplicate flags are move duplicate C "=3", it is judged that it is a duplicate of a license and it shifts to Step S350, without performing Step S348.

[0236]With reference to drawing 20, the enciphering processing part 5217, By open encryption key KPmc4 [peculiar to the license management device 520 obtained by the decoding processing section 5212], a license is enciphered and encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc4 is generated (Step S350). And the update date CRLdate of the prohibition class lists transmitted from the memory card 110. When the license management device 520 is compared with the update date of the prohibition class lists currently held to the CRL field 5215A, it is judged whether which prohibition class lists are new and the direction of MEMOKADO 100 is judged to be new, it shifts to Step S350. When the direction of the license management device 520 is judged to be new, it shifts to Step S362 (Step S352).

[0237]When the direction of the memory card 110 is judged to be new, the enciphering processing part 5206, Encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc4 outputted from the enciphering processing part 5217 is enciphered by session key Ks2 generated in the session key generating part 5218, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 is outputted to bus BS5. And the controller 5220, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 on bus BS5 is transmitted to the personal computer 50 via the interface 5224 and the terminal 5226 (Step S354).

[0238]The controller 510 of the personal computer 50, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 is received, and it transmits to the reproduction terminal 102 via USB interface 550, the terminal 580, and USB cable 70 (Step S356).

[0239]The controller 1106 of the reproduction terminal 102 receives encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 via terminal 1114, USB interface 1112, and bus BS3, The encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 which received is transmitted to the memory card 110 via bus BS3 and the memory card interface 1200. And the controller 1420 of the memory card 110 receives encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 via the terminal 1426, the interface 1424, and bus BS4 (Step S358).
[0240]The decoding processing section 1412 of the memory card 110, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 is received via bus BS4, It decodes by session key Ks2 generated by the session key generating part 1418, and {transaction ID// content ID//Kc//ACm//ACp} Kmc4 is received (Step S360). Then, it shifts to Step S374 shown in drawing 21.
[0241]When the direction of the license management device 520 is judged to be new, on the other hand in Step S350, the controller 5220 of the license management device 520, The data CRL of the newest prohibition class lists is acquired from the CRL field 5215A of the memory 5215 via bus BS5 (Step S362).
[0242]The enciphering processing part 5206 the output of the enciphering processing part 5217, and the data CRL of the prohibition class lists which the controller 5220 acquired from the memory 5215 via bus BS5, Respectively, it receives via the change-over switches 5242 and 5246, and enciphers by session key Ks2 generated in the session key generating part 5218. Encryption data {CRL//{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 outputted from the enciphering processing part 5206, It is outputted to the personal computer 50 via bus BS5, the interface 5224, and the terminal 5226 (Step S364).
[0243]The controller 510 of the personal computer 50, Encryption data {CRL//{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 outputted is received, Encryption data {CRL//{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 is transmitted to the reproduction terminal 102 via USB interface 550, the terminal 580, and USB cable 70 (Step S366). The controller 1106 of the reproduction terminal 102 receives encryption data {CRL//{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 via terminal 1114, USB interface 1112, and bus BS3, Encryption data {CRL//{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 is transmitted to the memory card 110 via bus BS3 and the memory card interface 1200. And the controller 1420 of the memory card 110, Encryption data {CRL//{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 is received via the terminal 1426, the interface 1424, and bus BS4 (Step S368).
[0244]In the memory card 110, the decoding processing section 1412, The received data on bus BS4 are decoded using session key Ks2 given from the session key generating part 1418, and CRL and {transaction ID// content ID//Kc//ACm//ACp} Kmc4 are received (Step 370). The controller 1420 receives the data CRL received by the decoding processing section 1412 via bus BS4, and rewrites the CRL field 1415A of the memory 1415 with the received data CRL (Step S372).
[0245]Step S354, S356, S358, and S360, From the prohibition class lists CRL of the license management device 520 of the transmitting side. It is the moving operation to the memory cards 110, such as the license key Kc when the prohibition class lists CRL of the memory card 110 of a receiver are new, Step S362, S364, S366, S368, S370, and S372, It is the moving operation to the memory cards 110, such as the license key Kc when the prohibition class lists CRL of the license management device 520 of the transmitting side are newer than the prohibition class lists CRL of the memory card 110 of a receiver. By thus, the update date CRLdate spent from the memory card 110. The

outflow of the license to the apparatus by which the license was broken can be prevented by checking and making the newest prohibition class lists CRL store in the CRL field 1514A as the prohibition class lists CRL of the memory card 110 as much as possible in detail.

[0246]With reference to drawing 21, with directions of the controller 1420 after Step S360 or Step S372. Encryption license {transaction ID// content ID//Kc//ACm//ACp} Kmc4, In the decoding processing section 1404, it is decoded by secret decode key Kmc4 and a license (license key Kc, transaction ID, content ID, the access control information ACm, and reproduction control information ACp) is received (Step S374).

[0247]The controller 510 of the personal computer 50 transmits the entry number for storing the license which moved to the memory card 110 to the reproduction terminal 102 via USB interface 550, the terminal 580, and USB cable 70. So then, the controller 1106 of the reproduction terminal 102, An entry number is received via terminal 1114, USB interface 1112, and bus BS3, Transmit to the memory card 110 via bus BS3 and the memory card interface 1200, and the controller 1420 of the memory card 110, An entry number is received via the terminal 1426 and the interface 1424, To the license area 1415B of the memory 1415 specified with the received entry number. The license (license key Kc, transaction ID, content ID, the access control information ACm, and reproduction control information ACp) acquired in Step S374 is stored (Step S378).

[0248]The controller 510 of the personal computer 50, The entry number of the license stored in the memory 1415 of the memory card 110, The license management file to enciphered content data {Dc} Kc and additional information Dc-inf which are going to move to the memory card 110 containing transaction ID and content ID of a plaintext is generated, and it transmits to the memory card 110 (Step S380).

[0249]The controller 1420 of the memory card 110 records the license management file which received the license management file via the reproduction terminal 102, and received to the data area 1415C of the memory 1415 (Step S382).

[0250]And the controller 510 of the personal computer 50, The inside of the license recorded on HDD530 according to judgment of Step S346 (Step S348) when it was movement, The license entry number of the license management file to the license which moved to the memory card 110 is eliminated, and it updates to nothing [license] (Step S386). Then, the controller 510 acquires from HDD530 enciphered content data {Dc} Kc and additional information Dc-inf which are going to move to the memory card 110, and transmits {Dc} Kc//Dc-inf to the memory card 110 (Step S390). The controller 1420 of the memory card 110, It records on the data area 1415C of the memory 1415 by making into a contents file {Dc} Kc//Dc-inf which received {Dc} Kc//Dc-inf via the reproduction terminal 102 (Step S392), and received via bus BS4 (Step S394).

[0251]If it does so, the controller 510 of the personal computer 50 will create the regenerated list which added the musical piece which moved to the memory card 110 (Step S396), and will transmit a regenerated list and rewriting directions of a regenerated list to the memory card 110 (Step S398). The controller 1420 of the memory card 110, A reproduction list file and rewriting directions are received via the reproduction terminal 102 (Step S400), It rewrites to the reproduction list file which received the reproduction list file recorded on the data area 1415C of the memory 1415 via bus BS4 (Step S402), and moving operation is completed (Step S404).

[0252]Thus, after checking that the memory card 110 with which the reproduction terminal 102 was equipped is regular apparatus, and that open encryption key KPm3 which has enciphered and transmitted with class certificate Cm3 is effective simultaneously, Class certificate Cm3 can move contents data only to the move demand to the memory card which is not written in prohibition class lists, i.e., the class

certificate list in which encryption by open encryption key KPm3 was broken, Movement using the class key to the inaccurate memory card moved and decoded can be forbidden.

[0253]By exchanging the encryption key generated with a license management device and a memory card, respectively, performing encryption using the encryption key which each received, and transmitting the encryption data to the other party, De facto mutual recognition can be performed also in transmission and reception of each encryption data, and enciphered content data and the security in the moving operation of a license can be raised.

[0254]Although it explained as moving processing that it was clear from explanation, when the duplicate of the license is permitted by the contents supplier, he performs as duplicate processing and a license is held as it is at the license management device 520 of the transmitting side. The duplicate in this case is an act permitted only when a contents supplier, i.e., a copyright person, permits a duplicate and he sets up movement / duplicate flags of the access control information ACm good [a move duplicate] at the time of distribution, and is not the act which checked the copyright person's right. Access control information is a part of license, and since the confidentiality is guaranteed, copyright is protected.

[0255]By using this moving operation, the user of the reproduction terminal 102 who does not have a communication function with the distributing server 10 can also receive enciphered content data and a license to a memory card via the personal computer 50, and his convenience of a user improves.

[0256]In the above, although movement of the license to the memory card 110 from the license management device 520 of the personal computer 50 was explained, Movement of a license to the license management device 520 from the memory card 110 is also performed according to the flow chart shown in drawing 18 - drawing 21. That is, in drawing 1, the portable telephone 100 will receive distribution and the enciphered content data and the license which were stored in the memory card 110 can be evacuated to the personal computer 50.

[0257]That the personal computer 50 can move the license received from the distributing server 10 to the memory card 110, The license management device 520 is only the license received in hard from the distributing server 10, The license management module 511 cannot transmit the enciphered content data and the license which were received in soft from the distributing server 10 to a memory card by the concept of "movement." The license management module 511 exchanges authentication data, an encryption key, etc. between the distributing servers 10 in soft with a security level lower than the license management device 520, Since enciphered content data and a license are received, a possibility that encryption will be broken in the receiving operation is higher than the case where the license management device 520 receives enciphered content data and a license. Therefore, the enciphered content data and the license which received with the low security level and were managed, Supposing it is freely movable to the memory card 110 which receives and manages enciphered content data and a license with the same security level as the license management device 520 by the concept of "movement", Since the security level in the memory card 110 falls, in order to prevent this, by the concept of "movement", it cannot transmit to the memory card 110 and the enciphered content data and the license which were received with the license management module 511 are carried out.

[0258]However, entirely, supposing the enciphered content data and the license with a low security level which were received with the license management module 511 are immovable to the memory card 110, It is contrary to the meaning of a data distribution system of permitting the free copy of contents data, protecting copyright, and a user's

convenience does not improve, either. Then, it enabled it to transmit the enciphered content data and the license which were received with the license management module 511 to the memory card 110 by the concept of the check-out explained below and check-in.

[0259][Check-out] In the data distribution system shown in drawing 1 and drawing 2, The operation which transmits the enciphered content data and the license which were distributed to the license management module 511 of the personal computer 50 from the distributing server 10 to the memory card 110 equipped by the reproduction terminal 102 is explained. This operation is called "check-out."

[0260]In the data distribution system which shows drawing 1 and drawing 2 drawing 22 - drawing 25, The license management module 511 the enciphered content data and the license which were received from the distributing server 10, They are the 1st for explaining the check-out operation which lends out enciphered content data and a license to the memory card 110 with which the reproduction terminal 102 was equipped on condition of return - the 4th flow chart. Since the portable telephone 100 or the reproduction terminal 102 is apparatus of only relaying data also in check-out, it has been omitted from the flow chart. In explaining, the case where it moves to the memory card 110 with which the reproduction terminal 102 of drawing 2 was equipped is explained, but the same may be said of the case where it moves to the memory card 110 with which the portable telephone 100 of drawing 1 was equipped, and reading ****** is good for the portable telephone 100 in the reproduction terminal 102.

[0261]Before the processing in drawing 20, the user of the personal computer 50 determines the contents to check out according to a contents list file, and explains as a premise that the contents file and the license management file can be specified.

[0262]If a check-out request is inputted from the keyboard 560 of the personal computer 50 with reference to drawing 22 (Step S500), the controller 510 will acquire encryption license data from the license management file recorded on HDD530. In this case, a license management file receives enciphered content data and a license with the license management module 511, and stores the encryption level 1 extension license which gave original encryption (step S266 reference of drawing 17). The license management module 511 acquires the encryption level 1 extension license of encryption license data to check out from a license management file, It decodes and a license (transaction ID, content ID, license key Kc, access-control-information ACm, reproduction control information ACp) and check-out information are acquired (Step S502).

[0263]The license management module 511 checks the access control information ACm (Step S504). That is, the license management module 511, Based on the acquired access control information ACm, the license which he is going to check out to the memory card 110 with which the reproduction terminal 102 was equipped by the access control information ACm. [whether there is any specification of the reproduction frequency of enciphered content data, and] It is checked whether it is the license whose reproduction is impossible. It is because there is no meaning which he checks out to the memory card 110 which it could not reproduce according to the license which checked out enciphered content data, but was equipped with the enciphered content data and license by the reproduction terminal 102 when reproduction has restriction.

[0264]In Step S504, when reproduction has restriction, it shifts to Step S588 and check-out operation is ended. In Step S504, when there is no restriction to reproduction, it shifts to Step S506. And it is checked whether the license management module 511 has a number larger than "0" which is contained in the acquired check-out information and which can be checked out (Step S506). In Step S506, since there will be no license which can already be checked out if the number which can be checked out is below "0", it shifts to Step S588 and check-out operation is ended. In Step S506, when the number

which can be checked out is larger than "0", the license management module 511 transmits the Request to Send of authentication data via USB interface 550, the terminal 580, and USB cable 70 (Step S508). The controller 1106 of the reproduction terminal 102 receives the Request to Send of authentication data via terminal 1114, USB interface 1112, and bus BS3, The Request to Send of authentication data which received is transmitted to the memory card 110 via bus BS3 and the memory card interface 1200. And the controller 1420 of the memory card 110 receives the Request to Send of authentication data via the terminal 1426, the interface 1424, and bus BS4 (Step S510).
[0265]The controller 1420 will read authentication data {KPm3//Cm3} KPa from the authentication data attaching part 1400 via bus BS4, if the Request to Send of authentication data is received, The read authentication data {KPm3//Cm3} KPa is outputted to the reproduction terminal 102 via bus BS4, the interface 1424, and the terminal 1426. And the controller 1106 of the reproduction terminal 102, Authentication data {KPm3//Cm3} KPa is received via the memory card interface 1200 and bus BS3, Authentication data {KPm3//Cm3} KPa is transmitted to the personal computer 50 via bus BS3, USB interface 1112, the terminal 1114, and USB cable 70 (Step S512).
[0266]So then, the license management module 511 of the personal computer 50, Authentication data {KPm3//Cm3} KPa is received via the terminal 580 and USB interface 550 (Step S514), and the authentication data {KPm3//Cm3} KPa which received is decoded with the authentication key KPa (Step S516). The license management module 511 from a decoding processing result. [whether processing was performed normally and] Namely, in order that the memory card 110 may attest holding class public presentation encryption key KPm3 from a regular memory card, and class certificate Cm3, Authenticating processing which judges whether the authentication data which gave the code for proving the justification in a regular organization was received is performed (Step S518). When it is judged that it is just authentication data, the license management module 511 recognizes and receives class public presentation encryption key KPm3 and class certificate Cm3. And it shifts to the next processing (Step S520). In not being just authentication data, it is considered as non approval, and it ends processing without receiving class public presentation encryption key KPm3 and class certificate Cm3 (Step S588).
[0267]Here, since the license management module 511 holds only the open authentication key KPb corresponding to level 1, a security level can perform only the check-out to level 1.
[0268]When it is recognized as a result of attestation that it is a regular memory card, the license management module 511, Next, when it refers for whether class certificate Cm3 of the memory card 110 is listed by the prohibition class lists CRL to HDD530 and these class certificates have been the targets of prohibition class lists about it, check-out operation is ended here (Step S588). On the other hand, when the class certificate of the memory card 110 is outside the object of prohibition class lists, it shifts to the next processing (Step S520).
[0269]If it is checked with reference to drawing 23 that it is access from the reproduction terminal provided with a memory card with just authentication data as a result of attestation, and a class is outside the object of prohibition class lists, The license management module 511 generates transaction ID for check-out which is the management codes for specifying check-out (Step S522). Transaction ID for check-out takes a certainly different value from all the transaction ID stored in the memory card 110, and generates it as transaction ID of local use. And the license management module 511 generates session key Ks22 for check-out (Step S524), and session key Ks22 generated is enciphered by class public presentation encryption key KPm3 transmitted from the memory card 110 (Step S526). And the license management

module 511, Transaction IDfor check-out//{Ks22} Km3 which added transaction ID for check-out to encryption data {Ks22} Km3 via USB interface 550, the terminal 580, and USB cable 70. It transmits to the reproduction terminal 102 (Step S528). So then, the controller 1106 of the reproduction terminal 102, Transaction IDfor check-out//{Ks22} Km3 are received via terminal 1114, USB interface 1112, and bus BS3, Its transaction IDfor check-out// {Ks22} Km3 which received are transmitted to the memory card 110 via the memory card interface 1200. And the controller 1420 of the memory card 110 receives transaction IDfor check-out//{Ks22} Km3 via the terminal 1426, the interface 1424, and bus BS4 (Step S530). The decoding processing section 1422 receives {Ks22} Km3 from the controller 1420 via bus BS4, by class secret decode key Km3 from the Km attaching part 1421, decodes {Ks22} Km3 and receives session key Ks22 (Step S532). And the session key generating part 1418 generates session key Ks2 (Step S534), and the controller 1420, The update date CRLdate of prohibition class lists is acquired from the CRL field 1415A of the memory 1415 via bus BS4, and the acquired update date CRLdate is given to the change-over switch 1446 (Step S536).

[0270]So then, session key Ks2 acquired when the enciphering processing part 1406 switched the terminal of the change-over switch 1446 one by one, individual public presentation encryption key KPmc4, and the update date CRLdate. It enciphers by session key Ks22 decoded by the decoding processing section 1404, and Ks2//KPmc4//encryption data {CRLdate} Ks22 are generated. The controller 1420 outputs Ks2//KPmc4//encryption data {CRLdate} Ks22 to the reproduction terminal 102 via bus BS4, the interface 1424, and the terminal 1426, The controller 1106 of the reproduction terminal 102 receives Ks2//KPmc4//encryption data {CRLdate} Ks22 via the memory card interface 1200. And the controller 1106 transmits to the personal computer 50 via USB interface 1112, the terminal 1114, and USB cable 70 (Step S538).

[0271]The license management module 511 of the personal computer 50, Ks2//KPmc4//encryption data {CRLdate} Ks22 are received via the terminal 580 and USB interface 550 (Step S540), Its Ks2//KPmc4// encryption data {CRLdate} Ks22 which received are decoded by session key Ks22, and session key Ks2, individual public presentation encryption key KPmc4, and the update date CRLdate are received (Step S542). And the license management module 511 generates the access control information ACm for check-out by which a license is not moved / reproduced to other memory cards from the memory card with which the reproduction terminal 102 was equipped. That is, the access control information ACm which made move reproduction of movement / duplicate flags of reproduction frequency indefinitely (=255) and improper (=3) is generated (Step S544).

[0272]With reference to drawing 24, the license management module 511, By open encryption key KPmc4 [peculiar to the license management module 511 received in Step S542]. A license is enciphered and encryption data [ACm / transaction ID/for check-out / content ID//Kc// / for check-out//] {ACp} Kmc4 is generated (Step S546). And the update date CRLdate of the prohibition class lists transmitted from the memory card 110. When it is compared with the update date of the prohibition class lists held HDD530 which the license management module 511 manages, it is judged whether which prohibition class lists are new and the direction of the memory card 110 is judged to be new, it shifts to Step S550. Conversely, when the license management module 511 is newer, it shifts to Step S556 (Step S548).

[0273]When the direction of the memory card 110 is judged to be new, the license management module 511, Encryption data [ACm / transaction ID/for check-out / content ID//Kc// / for check-out//] {ACp} Kmc4 is enciphered by session key Ks2, Transaction ID// content ID//Kc//encryption data {{ACm//ACpfor check-out for check-out} Kmc4} Ks2 via USB interface 550, the terminal 580, and USB cable 70. It

transmits to the reproduction terminal 102 (Step S550).
[0274]The controller 1106 of the reproduction terminal 102, Transaction ID// content ID//Kc//encryption data {{ACm//ACpfor check-out for check-out} Kmc4} Ks2 are received via terminal 1114, USB interface 1112, and bus BS3, Its transaction ID// content ID//Kc// encryption data {{ACm//ACpfor check-out for check-out} Kmc4} Ks2 which received are transmitted to the memory card 110 via bus BS3 and the memory card interface 1200. And the controller 1420 of the memory card 110, Transaction ID// content ID//Kc//encryption data {{ACm//ACpfor check-out for check-out} Kmc4} Ks2 are received via terminal 1426, terminal 1424, and bus BS4 (Step S552).
[0275]The decoding processing section 1412 of the memory card 110, Transaction ID// content ID//Kc//encryption data {{ACm//ACpfor check-out for check-out} Kmc4} Ks2 are received via bus BS4, It decodes by session key Ks2 generated by the session key generating part 1418, and transaction ID// content ID//Kc//{ACm//ACpfor check-out for check-out} Kmc4 are received (Step S554). Then, it shifts to Step S566 shown in drawing 25.
[0276]On the other hand, in Step S548, the prohibition class lists CRL with the newer prohibition class lists of the license management module 511 whose license management module 511 a license management module will manage from HDD530 if judged are acquired (Step S556).
[0277]And the license management module 511, Transaction ID// content ID//Kc//{ACm//ACpfor check-out for check-out} Kmc4, The data CRL of the prohibition class lists acquired from HDD530 is enciphered by session key Ks2, Its transaction ID// content ID//Kc// encryption data {CRL//{ACm//ACpfor check-out for check-out} Kmc4} Ks2 via USB interface 550, the terminal 580, and USB cable 70. It transmits to the reproduction terminal 102 (Step S558). The controller 1106 of the reproduction terminal 102, Transaction ID// content ID//Kc//encryption data {CRL//{ACm//ACpfor check-out for check-out} Kmc4} Ks2 are received via terminal 1114, USB interface 1112, and bus BS3, Its transaction ID// content ID//Kc// encryption data {CRL//{ACm//ACpfor check-out for check-out} Kmc4} Ks2 which received are outputted to the memory card 110 via bus BS3 and the memory card interface 1200. So then, the controller 1420 of the memory card 110, Transaction ID// content ID//Kc//encryption data {CRL//{ACm//ACpfor check-out for check-out} Kmc4} Ks2 are received via the terminal 1426, the interface 1424, and bus BS4 (Step S560).
[0278]In the memory card 110, the decoding processing section 1412, The received data on bus BS4 are decoded using session key Ks2 given from the session key generating part 1418, CRL, and transaction ID// content ID//Kc//{ACm//ACpfor check-out for check-out} Kmc4 are received (Step 560). The controller 1420 receives the data CRL received by the decoding processing section 1412 via bus BS4, and rewrites the CRL field 1415A of the memory 1415 with the received data CRL (Step S564).
[0279]Step S550, S552, and S554 from the prohibition class lists CRL of the license management module 511 of the transmitting side. It is check-out operation to the memory cards 110, such as the license key Kc when the prohibition class lists CRL of the memory card 110 of a receiver are new, Step S556, S558, S560, S562, and S564, It is check-out operation to the memory cards 110, such as the license key Kc when the prohibition class lists CRL of the license management module 511 of the transmitting side are newer than the prohibition class lists CRL of the memory card 110 of a receiver. By thus, the update date CRLdate of the prohibition class lists sent from the memory card 110. The outflow of the license to apparatus can be prevented by checking, acquiring the newest prohibition class lists CRL from HDD530 as much as possible in detail, and making it store in the CRL field 1514A as the prohibition class lists CRL of the memory card 110.

[0280]With reference to drawing 25, with directions of the controller 1420 after Step S554 or Step S564. Encryption license [ACm / transaction ID/for check-out / content ID//Kc// / for check-out//] {ACp} Kmc4, In the decoding processing section 1404, it is decoded by secret decode key Kmc4 and a license (license key Kc, transaction ID for check-out, content ID, ACm for check-out, and reproduction control information ACp) is received (Step S556).
[0281]Via USB interface 550, the terminal 580, and USB cable 70, the controller 510 of the personal computer 50 transmits to the reproduction terminal 102, and carries out the entry number for storing the license which moved to the memory card 110 (Step S567). So then, the controller 1106 of the reproduction terminal 102, An entry number is received via terminal 1114, USB interface 1112, and bus BS3, To the license area 1415B of the memory 1415 specified with the received entry number. The license (license key Kc, transaction ID for check-out, content ID, ACm for check-out, and reproduction control information ACp) acquired in Step S566 is stored (Step S568).
[0282]The controller 510 of the personal computer 50, The entry number of the license stored in the memory 1415 of the memory card 110, The license management file to enciphered content data {Dc} Kc and additional information Dc-inf which are going to move to the memory card 110 containing transaction ID for check-out and content ID of a plaintext is generated, It transmits to the memory card 110 (Step S569).
[0283]The controller 1420 of the memory card 110 receives a license management file via the reproduction terminal 102, and records the license management file which received on the data area 1415C of the memory 1415 (Step S570).
[0284]The license management module 511 of the personal computer 50, Subtract the number which can be checked out one time (Step S571), and Transaction ID, Content ID, check-out information which license-key-Kc(ed), access-control-information-ACm(ed), and it reproduction-control-information-ACp(ed), and was updated (with the number which can be checked out.) The new encryption level 1 extension license which gave the code original with what added individual public presentation encryption key KPmc4 of transaction ID for check-out and the memory card 110 of a check-out place is generated, Renewal record of the license data of the license management file recorded on HDD530 with the generated encryption license data is carried out (Step S572). Since individual public key KPmc4 of a check-out place is stored in the Tampa-proof module of a memory card, and it can be obtained by the high means of communication of the security using the code by attestation and has a characteristic value for every memory card, it is suitable as identification information which specifies a memory card.
[0285]The license management module 511 acquires from HDD530 enciphered content data {Dc} Kc and additional information Dc-inf which he is going to check out to the memory card 110, and transmits {Dc} Kc//Dc-inf to the memory card 110 (Step S574). The controller 1420 of the memory card 110, It records on the data area 1415C of the memory 1415 by making into a contents file {Dc} Kc//Dc-inf which received {Dc} Kc//Dc-inf via the reproduction terminal 102 (Step S576), and received via bus BS4 (Step S578).
[0286]So then, the license management module 511 of the personal computer 50, The regenerated list which added the musical piece checked out to the memory card 110 is created (Step S580), and a regenerated list and rewriting directions of a regenerated list are transmitted to the memory card 110 (Step S582). The controller 1420 of the memory card 110, A regenerated list and rewriting directions are received via the reproduction terminal 102 (Step S584), It rewrites to the reproduction list file which received the reproduction list file currently recorded on the data area 1415C of the memory 1415 via bus BS4 (Step S586), and check-out operation is completed (Step S588).

[0287]Thus, after checking that the memory card 110 with which the reproduction terminal 102 was equipped is regular apparatus, and that open encryption key KPm3 which has enciphered and transmitted with class certificate Cm3 is effective simultaneously, Class certificate Cm3 can check out contents data only to the check-out demand to the memory card which is not written in prohibition class lists, i.e., the class certificate list in which encryption by open encryption key KPm3 was broken, The check-out using the class key to the inaccurate memory card checked out and decoded can be forbidden.
[0288]By exchanging the encryption key generated with a license management module and a memory card, respectively, performing encryption using the encryption key which each received, and transmitting the encryption data to the other party, De facto mutual recognition can be performed also in transmission and reception of each encryption data, and enciphered content data and the security in check-out operation of a license can be raised.
[0289]The user of the reproduction terminal 102 who does not have a communication function with the distributing server 10 by using this check-out operation, The personal computer 50 can receive the enciphered content data and the license which were received in soft to a memory card, and convenience's of a user improves.
[0290][Check-in] Next, in the data distribution system shown in drawing 1 and drawing 2, The operation which returns the enciphered content data and the license by which he was checked out from the license management module 511 of the personal computer 50 to the memory card 110 to the license management module 511 is explained. This operation is called "check-in."
[0291]Drawing 26 - 28 are the 1st for explaining the check-in operation which returns and gets the enciphered content data and the license which were lent out to the memory card 110 by check-out operation explained with reference to drawing 22 - 25 - the 3rd flow chart. Since the portable telephone 100 or the reproduction terminal 102 is apparatus of only relaying data also in check-in, it has been omitted from the flow chart. The same may be said of the case where it moves from the memory card 110 with which the portable telephone 100 of drawing 1 was equipped, and what is necessary is to explain the case where it moves from the memory card 110 with which the reproduction terminal 102 of drawing 2 was equipped in explaining, but just to read the reproduction terminal 102 as the portable telephone 100.
[0292]Before the processing in drawing 26, the user of the personal computer 50 determines the contents at which he checks in according to a contents list file, and explains as a premise that the contents file and the license management file can be specified.
[0293]When a check-in request is inputted from the keyboard 560 of the personal computer 50 with reference to drawing 26 (Step S600), the license management module 511, Encryption level 1 extension license data are acquired from the license management file recorded on HDD530, decoding -- a license (transaction ID and content ID -- it license-key-Kc(ing) and) Access-control-information ACm, the reproduction control information ACp, and check-out information (individual public presentation encryption key KPmcx of the memory card of the number which can be checked out, transaction ID for check-out, and a check-out place) are acquired (Step S602). And the license management module 511 transmits the Request to Send of authentication data to the reproduction terminal 102 via USB interface 550, the terminal 580, and USB cable 70 (Step S604). So then, the controller 1106 of the reproduction terminal 102, The Request to Send of authentication data is received via terminal 1114, USB interface 1112, and bus BS3, and the Request to Send of authentication data is transmitted to the memory card 110 via bus BS3 and the memory card interface 1200.

And the controller 1420 of the memory card 110 receives the Request to Send of authentication data via the terminal 1426, the interface 1424, and bus BS4 (Step S606).
[0294]The controller 1420 will read authentication data {KPm3//Cm3} KPa from the authentication data attaching part 1400 via bus BS4, if the Request to Send of authentication data is received, The read authentication data {KPm3//Cm3} KPa is outputted to the reproduction terminal 102 via bus BS4, the interface 1424, and the terminal 1426. And the controller 1106 of the reproduction terminal 102, Authentication data {KPm3//Cm3} KPa is received via the memory card interface 1200 and bus BS3, Authentication data {KPm3//Cm3} KPa is transmitted to the personal computer 50 via bus BS3, USB interface 1112, the terminal 1114, and USB cable 70 (Step S608).
[0295]So then, the license management module 511 of the personal computer 50, Authentication data {KPm3//Cm3} KPa is received via the terminal 580 and USB interface 550 (Step S610), and the authentication data {KPm3//Cm3} KPa which received is decoded with the authentication key KPa (Step S612). And the license management module 511, In order that whether processing having been performed normally and the memory card 110 may attest holding class public presentation encryption key KPm3 from a regular memory card, and class certificate Cm3 from a decoding processing result, Authenticating processing which judges whether the authentication data which gave the code for proving the justification in a regular organization was received is performed (Step S614). When it is judged that it is just authentication data, the license management module 511 recognizes and receives class public presentation encryption key KPm3 and class certificate Cm3. And it shifts to the next processing (Step S616). In not being just authentication data, it is considered as non approval, and it ends processing without receiving class public presentation encryption key KPm3 and class certificate Cm3 (Step S670).
[0296]If it is recognized as a result of attestation that it is a regular memory card, the license management module 511 will generate straw-man transaction ID (Step S616). Transaction ID for straw men takes a certainly different value from all the transaction ID stored in the memory card 110, and is generated as transaction ID of local use. And the license management module 511, Session key Ks22 for check-in is generated (Step S618), Encipher by class public presentation encryption key KPm3 which received session key Ks22 generated from the memory card 110, and encryption data {Ks22} Km3 is generated (Step S620), Straw-man transaction ID//{Ks22} Km3 which added straw-man transaction ID to encryption data {Ks22} Km3 are transmitted to the reproduction terminal 102 via USB interface 550, the terminal 580, and USB cable 70 (Step S622).
[0297]With reference to drawing 27, the controller 1106 of the reproduction terminal 102, Straw-man transaction ID//{Ks22} Km3 are received via terminal 1114, USB interface 1112, and bus BS3, Its straw-man transaction ID// {Ks22} Km3 which received are transmitted to the memory card 110 via the memory card interface 1200. And the controller 1420 of the memory card 110 receives straw-man transaction ID//{Ks22} Km3 via the terminal 1426, the interface 1424, and bus BS4 (Step S624). The decoding processing section 1422 receives {Ks22} Km3 from the controller 1420 via bus BS4, by class secret decode key Km3 from the Km attaching part 1421, decodes {Ks22} Km3 and receives session key Ks22 (Step S626). And the session key generating part 1418 generates session key Ks2 (Step S628), and the controller 1420, The update date date of the prohibition class lists CRL is acquired from the CRL field 1415A of the memory 1415 via bus BS4, and the acquired update date CRLdate is given to the change-over switch 1446 (Step S630).
[0298]So then, session key Ks2 acquired when the enciphering processing part 1406 switched the terminal of the change-over switch 1446 one by one, individual public

presentation encryption key KPmc4, and the update date CRLdate. It enciphers by session key Ks22 which was decoded by the decoding processing section 1422 and acquired via terminal Pa of the change-over switch 1442, and Ks2//KPmc4//encryption data {CRLdate} Ks22 are generated. The controller 1420 outputs Ks2//KPmc4//encryption data {CRLdate} Ks22 to the reproduction terminal 102 via bus BS4, the interface 1424, and the terminal 1426, The controller 1106 of the reproduction terminal 102 receives Ks2//KPmc4//encryption data {CRLdate} Ks22 via the memory card interface 1200. And the controller 1106 transmits to the personal computer 50 via USB interface 1112, the terminal 1114, and USB cable 70 (Step S632).

[0299]The license management module 511 of the personal computer 50, Ks2//KPmc4//encryption data {CRLdate} Ks22 are received via the terminal 580 and USB interface 550 (Step S634), Its Ks2//KPmc4// encryption data {CRLdate} Ks22 which received are decoded by session key Ks22, and session key Ks2, individual public presentation encryption key KPmc4, and the update date CRLdate are received (Step S636).

[0300]So then, the license management module 511, Whether it is the no contained in the check-out information which individual public presentation encryption key KPmc4 received acquired from the license management file recorded on HDD530, That is, it is checked whether it is in agreement with the individual public presentation encryption key KPmcx stored corresponding to transaction ID for check-out of the license which he is going to check out (Step S638). This individual public presentation encryption key KPmc4 is contained in the check-out information updated on the occasion of check-out of enciphered content data and a license (see Step S572 of drawing 25). Therefore, the check-out place checked out on the occasion of check-in can be easily specified by including individual public presentation encryption key KPmc4 corresponding to check-out places, such as enciphered content data, in check-out information.

[0301]In Step S638, when individual public presentation encryption key KPmc4 is not contained in check-out information, check-in operation is ended (Step S670). When individual public presentation encryption key KPmc4 is contained in check-out information, in Step S638 the license management module 511, the straw-man license (straw-man transaction ID.) containing straw-man transaction ID Straw-man content ID, the straw man Kc, the straw man ACm, and the straw man ACp are enciphered by individual public presentation encryption key KPmc4, Straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/encryption data {/straw-man ACp} Kmc4 is generated (Step S640).

[0302]The license management module 511 enciphers straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/encryption data {/straw-man ACp} Kmc4 by session key Ks2, Straw-man transaction ID// straw-man content ID// dummy-keys Kc//straw-man ACm/encryption data {{/straw-man ACp} Kmc4} Ks2 is generated, The straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/encryption data {{/straw-man ACp} Kmc4} Ks2 generated via USB interface 550, the terminal 580, and USB cable 70. It transmits to the reproduction terminal 102 (Step S642).

[0303]The controller 1106 of the reproduction terminal 102, Straw-man transaction ID// straw-man content ID// straw-man license key Kc//straw-man ACm/encryption data {{/straw-man ACp} Kmc4} Ks2 is received via terminal 1114, USB interface 1112, and bus BS3. The controller 1106, Straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/encryption data {{/straw-man ACp} Kmc4} Ks2 which received is transmitted to the memory card 110 via bus BS3 and the memory card interface 1200. And the controller 1420 of the memory card 110, Straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/{{/straw-man ACp}

Kmc4} Ks2 is received via the terminal 1426, the interface 1424, and bus BS4 (Step S644).

[0304]With reference to drawing 28, the decoding processing section 1412 of the memory card 110, Straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/{{/straw-man ACp} Kmc4} Ks2 is received via bus BS4, It decodes by session key Ks2 generated by the session key generating part 1418, and straw-man transaction ID// straw-man content ID//Kc// straw-man ACm/{/straw-man ACp} Kmc4 is received (Step S646). And the decoding processing section 1404 receives straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/encryption data {/straw-man ACp} Kmc4 from the decoding processing section 1412, The straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/encryption data {/straw-man ACp} Kmc4 received is decoded by individual secret decode key Kmc4 from the Kmc attaching part 1402, A straw-man license (straw-man transaction ID, straw-man content ID, the straw man Kc, the straw man ACm, and straw man ACp) is received (Step S648).

[0305]The controller 510 of the personal computer 50, An entry number is acquired from the license management file corresponding to the checked-out license which is recorded on the data area 1415C of the memory card 110, As an entry number for storing a straw-man license, it transmits to the reproduction terminal 102 via USB interface 550, the terminal 580, and USB cable 70 (Step S649). So then, the controller 1106 of the reproduction terminal 102, An entry number is received via terminal 1114, USB interface 1112, and bus BS3, To the license area 1415B of the memory 1415 specified with the received entry number. The straw-man license (straw-man transaction ID, straw-man content ID, the straw man Kc, the straw man ACm, and straw man ACp) acquired in Step S648 is stored in the entry as which the license area 1415B of the memory 1415 was specified (Step S650). Thus, the license checked out to the memory card 110 is eliminable by overwriting to the license which wants to check in at a straw-man license.

[0306]Then, the license management module 511 of the personal computer 50, Only 1 increases the number within check-out information which can be checked out, individual public key KPmc4 of the memory card of transaction ID for check-out and a check-out place is deleted, and check-out information is updated (Step S652). And the license management module 511, Transaction ID, content ID, license key Kc, the access control information ACm, And encryption original with the reproduction control information ACp and the updated check-out information is given, encryption license data are created, and renewal record of the license data of the license management file recorded on HDD530 is carried out (Step S654).

[0307]So then, the license management module 511, The contents file (enciphered content data {Dc} Kc and additional information Dc-inf) and license management file to the checked-out license which is recorded on the data area 1415C of the memory 1415 of the memory card 100. The deletion instruction to delete is transmitted to the reproduction terminal 102 via USB interface 550, the terminal 580, and USB cable 70 (Step S656). The controller 1106 of the reproduction terminal 102 receives the deletion instruction of a contents file (enciphered content data {Dc} Kc and additional information Dc-inf) and a license management file via terminal 1114, USB interface 1112, and bus BS3, The deletion instruction of the contents file (enciphered content data {Dc} Kc and additional information Dc-inf) which received via bus BS3 and the memory card interface 1200, and a license management file is outputted to the memory card 110. So then, the controller 1420 of the memory card 110, The deletion instruction of a contents file (enciphered content data {Dc} Kc and additional information Dc-inf) and a license management file is received via the terminal 1426, the interface 1424, and

bus BS4 (Step S658). And the controller 1420 deletes the contents file (enciphered content data {Dc} Kc and additional information Dc-inf) and license management file which were recorded on the data area 1415C of the memory 1415 via bus BS4 (Step S660).

[0308]The license management module 511 of the personal computer 50 creates the regenerated list which deleted the musical piece at which he checked in (Step S662), and transmits a regenerated list and rewriting directions of a regenerated list to the memory card 110 (Step S664). The controller 1420 of the memory card 110, A reproduction list file and rewriting directions are received via the reproduction terminal 102 (Step S666), It rewrites to the reproduction list file which received the reproduction list file of the data area 1415C of the memory 1415 via bus BS4 (Step S668), and check-in operation is completed (Step S670).

[0309]Thus, by returning and getting enciphered content data and a license from the partner point which checked out enciphered content data and a license, A license from the license management module with a low security level in which movement is forbidden, Since the license which it was lent out to the memory card with a high security level, and was acquired by the license management module with a low security level in the memory card is receivable, Enciphered content data can be reproduced and enjoyed according to the license acquired by the license management module with a low security level in the reproduction terminal.

[0310]The license lent out to the memory card, Since it is specified that it cannot output the license which checked out the memory card to other recording devices (a memory card, a license management device, and a license management module) by the access control information ACm, the lent-out license does not flow out. By checking in to the lent-out license management module (return), the right of the lent-out license returns to the lent-out license management module. Therefore, a duplicate is not allowed to be made against an author's will, it is not the processing to which a security level falls, and copyright is also protected.

[0311][Reproduction] Next, the reproduction motion in the reproduction terminal 100 (it is [the following called contents playback device] the same) of the contents data in which he was checked out by the memory card 110 with reference to drawing 29 and drawing 30 is explained. Before the processing in drawing 29, the user of the reproduction terminal 102, The contents (musical piece) to reproduce are determined according to the regenerated list currently recorded on the data area 1415C of the memory card 100, a contents file is specified, and it explains acquiring the license management file as a premise.

[0312]With reference to drawing 29, reproduction instruction is inputted to the reproduction terminal 100 via the navigational panel 1108 with the start of reproduction motion from the user of the reproduction terminal 100 (Step S700). If it does so, the controller 1106 will read authentication data {KPp1//Cp1} KPa from the authentication data attaching part 1500 via bus BS3, Authentication data {KPp1//Cp1} KPa is outputted to the memory card 110 via the memory card interface 1200 (Step S702).

[0313]If it does so, the memory card 110 will receive authentication data {KPp1//Cp1} KPa (Step S704). And the decoding processing section 1408 of the memory card 110, Received authentication data {KPp1//Cp1} Decoding KPa with the open authentication key KPa held at the KPa attaching part 1414 (Step S706) the controller 1420 performs authenticating processing from the decoding processing result in the decoding processing section 1408. That is, authentication data {KPp1//Cp1} KPa performs authenticating processing which judges whether it is regular authentication data (Step S708). When it is not able to decode, it shifts to Step S748 and reproduction motion is ended. When authentication data is able to be decoded, it is judged whether the

controller 1420 is contained in the prohibition class lists CRL which certificate Cm1 acquired read from the CRL field 1415A of the memory 1415 (Step S710). In this case, the identification number is given to class certificate Cp1 and the controller 1420 distinguishes whether the identification number of received class certificate Cp1 exists in prohibition class-lists data. If it is judged that class certificate Cp1 is contained in prohibition class-lists data, it will shift to Step S748 and reproduction motion will be ended.

[0314]In Step S710, if it is judged that class certificate Cp1 is not contained in the prohibition class-lists data CRL, the session key generating part 1418 of the memory card 110 will generate session key Ks2 for reproduction sessions (Step S712). And the cipher-processing part 1410 outputs {Ks2} Kp1 which enciphered session key Ks2 from the session key generating part 1418 by open encryption key KPp1 decoded by the decoding processing section 1408 to bus BS3 (Step S714). If it does so, the controller 1420 will output {Ks2} Kp1 to the memory card interface 1200 via the interface 1424 and the terminal 1426 (Step S716). The controller 1106 of the reproduction terminal 100 acquires {Ks2} Kp1 via the memory card interface 1200. And the Kp1 attaching part 1502 outputs secret decode key Kp1 to the decoding processing section 1504.

[0315]By secret decode key Kp1 which was outputted from the Kp1 attaching part 1502 and which is open encryption key KPp1 and a pair, the decoding processing section 1504 decodes {Ks2} Kp1, and outputs session key Ks2 to the cipher-processing part 1506 (Step S718). If it does so, the session key generating part 1508 will generate session key Ks3 for reproduction sessions, and will output session key Ks3 to the cipher-processing part 1506 (Step S720). The cipher-processing part 1506 enciphers session key Ks3 from the session key generating part 1508 by session key Ks2 from the decoding processing section 1504, and outputs {Ks3} Ks2, The controller 1106 outputs {Ks3} Ks2 to the memory card 110 via bus BS3 and the memory card interface 1200 (Step S722).

[0316]If it does so, the decoding processing section 1412 of the memory card 110 will input {Ks3} Ks2 via the terminal 1426, the interface 1424, and bus BS4 (Step S724).

[0317]With reference to drawing 30, the decoding processing section 1412 decodes {Ks3} Ks2 by session key Ks2 generated by the session key generating part 1418, and receives session key Ks3 generated with the reproduction terminal 100 (Step S726).

[0318]The controller 1106 of a reproduction terminal acquires the entry number in which the license is stored from the license management file of the reproduction request song beforehand acquired from the memory card 110, The entry number acquired to the memory card 110 via the memory card interface 1200 is outputted (Step S727).

[0319]In the controller 1420, an entry number checks the access restriction information ACm according to an input (Step S728).

[0320]In Step S728, by checking the access restriction information ACm which is information about the restriction to access of a memory, specifically, By checking reproduction frequency, it ends reproduction motion, in being in a state [that it is already unreproducible], and when the reproduction frequency of access restriction information has restriction, it progresses to the following step, after [which reduces the reproduction frequency of the access restriction information ACm updating <1] carrying out (Step S730). On the other hand, when reproduction is not restricted by the reproduction frequency of the access restriction information ACm, Step S730 is skipped, and processing advances to the following step (Step S732), without updating the reproduction frequency of the access restriction information ACm.

[0321]In Step S728, when it is judged that it is renewable in the reproduction motion concerned, the license key Kc and the reproduction control information ACp of a reproduction request song which were recorded on the license area 1415B of the

memory 1415 are outputted on bus BS4 (Step S732).
[0322]The license key Kc and the reproduction control information ACp which were acquired are sent to the enciphering processing part 1406 via the point of contact Pf of the change-over switch 1446. The enciphering processing part 1406 enciphers the license key Kc and the reproduction control information ACp which were received via the change-over switch 1446 by session key Ks3 received from the decoding processing section 1412 via the point of contact Pb of the change-over switch 1442, {Kc//ACp} Ks3 is outputted to bus BS4 (Step S734).
[0323]The encryption data outputted to bus BS4 is sent out to the reproduction terminal 100 via the interface 1424, the terminal 1426, and the memory card interface 1200.
[0324]In the reproduction terminal 100, the decoding processing section 1510 performs decoding processing for encryption data [Kc//] {ACp} Ks3 transmitted to bus BS3 via the memory card interface 1200, and the license key Kc and the reproduction control information ACp are received (Step S736). The decoding processing section 1510 transmits the license key Kc to the decoding processing section 1516, and outputs the reproduction control information ACp to bus BS3.
[0325]Via bus BS3, the controller 1106 receives the reproduction control information ACp, and checks reproductive propriety (Step S740).
[0326]In Step S740, when it is judged by the reproduction control information ACp that reproduction is impossible, reproduction motion is ended.
[0327]When it is judged in Step S740 that it is refreshable, the controller 1106 requires enciphered content data {Dc} Kc of the memory card 110 via the memory card interface 1200. If it does so, the controller 1420 of the memory card 110 will acquire enciphered content data {Dc} Kc from the memory 1415, and will output it to the memory card interface 1200 via bus BS4, the interface 1424, and the terminal 1426 (Step S742).
[0328]The controller 1106 of the reproduction terminal 100 acquires enciphered content data {Dc} Kc via the memory card interface 1200, and gives enciphered content data {Dc} Kc to the decoding processing section 1516 via bus BS3.
[0329]And the decoding processing section 1516 decodes enciphered content data {Dc} Kc with the license key Kc outputted from the decoding processing section 1510, and acquires the contents data Dc (Step S744).
[0330]And the decoded contents data Dc is outputted to the music reproduction section 1518, the music reproduction section 1518 reproduces contents data, and DA converter 1519 changes a digital signal into an analog signal, and it outputs it to the terminal 1530. And from the terminal 1530, via an external output device, music data is outputted to the head telephone 130, and is reproduced (Step S746). Reproduction motion is completed by this.
[0331]Although the case where the enciphered content data recorded on the memory card 110 was reproduced with the reproduction terminal 100 in the above was explained, It is possible to reproduce the enciphered content data received by the license management module 511 and the license management device 520 by building the contents playback device 1550 shown in drawing 7 in the personal computer 50.
[0332]With reference to drawing 31, management of the enciphered content data received by the license management module 511 or the license management device 520 of the personal computer 50 and a license is explained. HDD530 of the personal computer 50 is provided with the following.
Contents list file 150.
Contents files 1531-1535.
License management files 1521-1525.

[0333]The contents list file 150 is a data file of the list form of contents to own, and the

information (file name) etc. which show each information over contents, including a musical piece name, an artist name, etc., and a contents file and a license management file are included. The information over each contents acquires required information from additional information Dc-inf at the time of reception, and is automatically indicated by a user's directions. Only a contents file can be managed in a list also about the contents which cannot reproduce only a license management file.
[0334]The contents files 1531-1535 are files which record enciphered content data {Dc} Kc received by the license management module 511 or the license management device 520, and additional information Dc-inf, and are provided for every contents.
[0335]The license management files 1521-1525 are files for managing the license which is recorded corresponding to the contents files 1531-1535, and was received by the license management module 511 or the license management device 520, respectively. A license cannot usually be referred to so that clearly [old explanation], but if other information except the license key Kc cannot even perform that a user rewrites, it is satisfactory in respect of copyright protection. However, since it leads to the fall of security, it is not preferred to separate from the license key Kc and to manage in employment. Then, when receiving license distribution, the copy of the matter restricted by transaction ID and content ID which can be referred to in a plaintext, and the access control information ACm and the reproduction control information ACp which can be easily judged from the license terms of purchase AC is recorded in a plaintext. When a license is recorded on the license management device 520, about the license which is under management of the license management module 511 about an entry number, an encryption level 1 extension license (a license and tic out information) is recorded. Original encryption according [an encryption level 1 extension license] to the license management module 511 is given. With original encryption. The personal computer 50 obtained from the personal computers 50, such as a version number etc. of BIOS which is a boot program of the number which the controller (CPU) of the personal computer 50 has individually, or a personal computer. It enciphers by relating with the information which can be specified. Therefore, the encryption level 1 generated license turns into a license original with the personal computer 50, and even if reproduced, it does not have a meaning with other devices. The license area 525B of the memory 5215 of the license management device 520 is a record section which comprised a Tampa-proof module which records a license with a high security level (level 2). It has N entries, in order to record a license (license key Kc, the reproduction control information ACp, access-restriction-information ACm, license ID).
[0336]With reference to drawing 31, the license management file 1521-1524 contains the entry numbers 0 and 1, respectively. the license (license ID.) which this is received by the license management device 520 and managed in the license area 5215B of the memory 5215 of the license management device 520 It is a number which specifies the management domain of license key Kc, the access control information ACm, and the reproduction control information ACm, and is a file concerning level 2 license.
[0337]When moving the enciphered content data of the file name recorded on the contents file 1531 to the memory card 110 equipped by the portable telephone 100 or the reproduction terminal 102, It is a solution or ** where if the contents files 1531-1535 are searched and the contents file 1531 is extracted, the license which reproduces enciphered content data is managed. Since the entry number contained in the license management file 1521 corresponding to the contents file 1531 is "0", The license which reproduces the enciphered content data of the file name recorded on the contents file 1531 is recorded on the field specified with the entry number 0 of the license area 5215B of the memory 5215 of the license management device 520. If it does so, the entry number 0 will be read from the license management file 1521 of the contents list

file 150 recorded on HDD530, By inputting the read entry number 0 into the license management device 520, a license is easily taken out from the license area 5215B of the memory 5215, and it can move to the memory card 110. And since the license in the entry number specified in the license area 5215B of the memory 5215 is deleted after moving a license (Step S354 of drawing 20, S366 reference), Corresponding to it, "nothing [license]" is recorded like the license management file 1523 (step S386 reference of drawing 21).

[0338]The license management file 1523 contains "nothing [license]." This is the result of moving the license received by the license management device 520. The corresponding contents file 1533 remains recorded on HDD530. It is possible to receive distribution from a memory card only about a license, when distribution is again licensed from movement or the distributing server 10 to the license management module 520.

[0339]The license of the enciphered content data received with the license management module 511 is managed by the license management file 1522-1525. The license management file 1522-1525 includes the license for reproducing the enciphered content data received with the license management module 511 (step S278 reference of drawing 17). As mentioned above, this the license management module 511, Since enciphered content data and a license are received in soft, it does not manage by writing a license in the license management device 520, but will record on HDD530 as a file.

[0340]When making it check out to the memory card 110 equipped with the enciphered content data of the file name recorded on the contents file 1533 by the reproduction terminal 102 so, then, for example, The contents files 1531-1535 can be searched, the contents file 1533 can be extracted, and check-out information, a license, etc. can be read from the license management file 1523 corresponding to the contents file 1533.

[0341]Thus, in this invention, the enciphered content data and the license which were received with the license management module 511, and the enciphered content data and the license which were received with the license management device 520 are managed in the same format. That is, it manages by the format which unified the enciphered content data and the license which were received with a different security level (level 1, level 2). Enciphered content data can be reproduced freely, protecting copyright, without reducing each security level, even when enciphered content data and a license are received with a different security level by doing in this way.

[0342]Drawing 32 shows the data area 1415C and the license area 1415C in the memory 1415 of the memory card 110. The reproduction list file 160, the contents files 1611-161n, and the license management files 1621-162n are recorded on the data area 1415C. The contents files 1611-161n record enciphered content data {Dc} Kc and additional information Dc-inf which received as one file. The license management files 1621-162n are recorded corresponding to the contents files 1611-161n, respectively.

[0343]When the memory card 110 receives enciphered content data and a license from the distributing server 10, When a "move session" or a "check-out session" receives enciphered content data and a license from the personal computer 50, enciphered content data and a license are recorded on the memory 1415. That is, the memory card 110 manages enciphered content data and a license on a hard target (a high security level is meant) regardless of a security level.

[0344]Therefore, it is received by the license management device 520 of the personal computer 50, And the license of the enciphered content data with a high security level transmitted to the memory card 110 by the move session, With the license of the enciphered content data with a low security level which was received by the license management module 510 and transmitted to the memory card 110 by the check-out session. If the license management file of the reproduction list file 160 which was

recorded on the field specified with the entry number of the license area 1415B of the memory 1415, and was recorded on the data area 1415C of the memory 1415 is read, An entry number can be acquired and a license corresponding with the acquired entry number can be read from the license area 1415B.
[0345]Although the license management file 1622 is shown by the dotted line, it shows what is not recorded actually. Although it means that there is no license and it cannot be reproduced although the contents file 1612 exists, this corresponds, for example, when a reproduction terminal receives only enciphered content data from other portable telephones.
[0346]Although the contents file 1613 is shown by the dotted line, As for this, a reproduction terminal receives enciphered content data and a license from the distributing server 10, for example, Although it corresponds when only the received enciphered content data is transmitted to other portable telephones, and a license exists in the memory 1415, it means that enciphered content data does not exist.
[0347][Ripping] The user of the personal computer 50 can acquire and use music data from the audio CD which enciphered content data and a license are acquired by distribution, and also is owned. Although digital reproduction of an audio CD may not be freely performed from the position of an owner's of a copyright right protection, he is allowed for an individual to reproduce using a tool provided with a copyright protection function for the self purpose of use, and to enjoy music. Then, the license management module 511 acquires music data from an audio CD, and also includes the program which realizes the ripping function which generates enciphered content data manageable by the license management module 511, and a license.
[0348]There are some which inserted digital watermarking called a watermark in music data in an audio CD in recent years. The range of the use in a user is written in this watermark by the owner of a copyright as a use rule. It is necessary to certainly follow this use rule from a point of copyright protection in ripping from the music data in which the use rule is written in. Henceforth, it is assumed that the reproduction frequency restrictions and available time over duplicate conditions <duplication prohibition, and the generation and duplicate which can be reproduced are possible>, the shelf-lives of a duplicate, the number of the maximum check-out, edit, reproduction speed, the code of a refreshable area, and a duplicate are indicated as a use rule. When a watermark is not detected, there is also the conventional audio CD in which the use rule is not written.
[0349]Ripping may digitize the music signal which music data was acquired directly and also was inputted as an analog signal, and may acquire it from an audio CD as music data. In order to reduce data volume, it is also possible to consider as an input the music data by which compression encoding was carried out. It is also possible to incorporate as an input the contents data distributed with distribution systems other than the distribution system by this embodiment.
[0350]With reference to drawing 33 and drawing 34, acquisition of the enciphered content data based on ripping from the audio CD on which music data was recorded, and a license is explained.
[0351]Drawing 33 is a functional block diagram showing the function of the software which carries out ripping of the music data which CD-ROM drive 540 contained in the personal computer 50 shown in drawing 6 read from CD. The software which carries out ripping of the music data is provided with the following.
Watermark detection means 5400.
Watermark judging means 5401.
Remark means 5402.
The license generating means 5403, the music encoder 5404, and the cryptographer

stage 5405.

[0352]The watermark detection means 5400 detects a watermark from the music data acquired from the audio CD, and extracts the use rule indicated. The watermark judging means 5401 judges the propriety of ripping based on the use rule indicated with the watermark, when it is able to be detected further whether it has detected as a result of [of the watermark detection means 5400] detection (i.e., a watermark). . In this case, when ripping is good, there is no use rule of a watermark. Or it means that the use rule to which the duplicate and movement of music data which were recorded on the audio CD were permitted was recorded with the watermark, When ripping is improper, it means that the use rule which must not reproduce and move the music data recorded on the audio CD was recorded with the watermark.

[0353]Ripping is possible for a decision result [in / in the remark means 5402 / the watermark judging means 5401], When there are directions of duplicate generations (i.e., when music data may be reproduced and moved), the watermark contained in music data is changed for the watermark which changed the duplicate conditions of music data. However, when considering as an input the music data coded when ripping of the analog signal was inputted and carried out, and in considering the music data distributed with other distribution systems as an input, if ripping is possible, it will not be concerned with the contents of the use rule, but will certainly change a watermark. In this case, when there are directions of duplicate generations, the contents of the use rule are changed, and when other, the acquired use rule is used as it is.

[0354]The license generating means 5403 generates a license based on the decision result of the watermark judging means 5401. The music encoder 5404 codes the music data in which the remark of the watermark was carried out to a prescribed method by the remark means 5402. The cryptographer stage 5405 enciphers the music data from the music encoder 5404 with the license key Kc contained in the license generated by the license generating means 5403.

[0355]With reference to drawing 34, the ripping operation in the controller 510 of the personal computer 50 is explained. If ripping operation is started, the watermark detection means 5400 will detect the use rule of a watermark based on the data detected from the audio CD (Step S800). And it is judged whether the watermark judging means 5401 can be reproduced based on the use rule currently recorded as the detection result and watermark of the watermark detection means 5400 (Step S802). A watermark is detected, and when a duplicate is permitted under a use rule and the contents of the use rule can respond in the access control information and reproduction control information within a license, it is judged that ripping is good and it shifts to Step S804. When a watermark is detected and the use rule [that it cannot respond in the access control information or reproduction control information within prohibition of a duplicate or a license] is indicated by the use rule, it is judged as prohibition of ripping, it shifts to Step S828, and ripping operation is ended. When the watermark is not contained in CD with which it was equipped, it shifts to Step S810.

[0356]In Step S802, when it is judged that ripping is good, music data is incorporated from an audio CD and the watermark contained in music data by the remark means 5402 is changed for the watermark which changed duplicate conditions (Step S806). That is, duplicate generations are changed for the watermark made into 2 times when the use rule of a watermark has permitted the duplicate up to three generations. And the license generating means 5403 generates the license reflecting a use rule. That is, the license generating means 5403 generates the license whose number of times of a duplicate is two generations (Step S806). Then, the license generating means 5403 generates the check-out information containing the number reflecting a use rule which

can be checked out (Step S808). About the number which can be checked out, when unstated, it is referred to as "3."
[0357]On the other hand, in Step S802, when a watermark is not detected, the license generating means 5403 generates the license which forbade the duplicate and movement of the license (Step S810). Then, the license generating means 5403 generates the check-out information in which an initial value contains the number which is 3, and which can be checked out (Step S812).
[0358]After Step S808 or S812, a watermark agreement-izes the music data by which the remark was carried out to a prescribed method, and the music encoder 5404 generates contents data {Dc} (Step S814). And the cryptographer stage 5405 enciphers with the license key Kc contained in the license generated by the license generating means 5403 in the music data from the music encoder 5404, and generates enciphered content data {Dc} Kc (Step S816). Then, additional information Dc-inf of contents data {Dc} is generated by the user input etc. which were inputted from the keyboard 560 of the information included in an audio CD, or the personal computer 50 (Step S818).
[0359]If it does so, the controller 510 of the personal computer 50 will acquire enciphered content data {Dc} Kc and additional information Dc-inf via bus BS2, and will record them on HDD530 (Step S822). And the controller 510 generates the encryption extension license which gave encryption original with the license (transaction ID, the content ID, license key Kc, access-restriction-information ACm, reproduction control information ACp) and check-out information which were generated (Step S822). Then, the controller 510 contains an encryption extension license, and transaction ID and content ID of a plaintext, And the license management file to enciphered content data {Dc} Kc and additional information Dc-inf which were recorded on HDD is generated, and it records on HDD530 (Step S824). Finally, the controller 510 adds the file name of the contents received to the contents list file currently recorded on HDD530 (Step S826), and ripping operation ends it (Step S828).
[0360]Thus, the license which could acquire enciphered content data and a license and was acquired from the audio CD by ripping is protected and managed with the contents distributed from the distributing server 10.
[0361]With reference to drawing 35 - 37, generation of the license in Step S806 of the flow chart shown in drawing 34 is explained in detail. As a license the license generating means 5403 Content ID, Transaction ID, a license key, access restriction information (restriction to the output of the license key in the memory card 110), reproduction control information (reproduction condition in the contents playback device 1550), and the number that can be checked out are generated.
[0362]With reference to drawing 35, the content ID 1 comprises the fixed area 2 and the management domain 3. Content ID comprises 16bytes, before long, 1 byte is assigned to the fixed area 2 and 15bytes is assigned to the management domain 3. And the fixed area 2 shows where the content ID 1 was generated, and a different value is written in by the case where it is generated by the case where content ID is generated by the distributing server 10, and the personal computer 50. When content ID is generated in the personal computer 50, That is, when content ID is generated locally, "00" is written in the fixed area 2 by the hexadecimal notation, and when content ID is generated except personal computer 50, the other value is written in the fixed area 2.
[0363]The identification number for identifying each contents data is written in, and the management domain 3 is managed so that one identification number may overlap and may not be attached to two or more contents data.
[0364]With reference to drawing 36, transaction ID4 comprises the fixed area 5 and the management domain 6. Transaction ID comprises 12bytes, before long, 1 byte is assigned to the fixed area 5 and 11bytes is assigned to the management domain 6. And

the fixed area 5 comprises the fixation flag 7 and the reserve field 8. 1 bit is assigned to the fixation flag 7 and 7bits is assigned to the reserve field 8. The fixation flag 7 shows for what kind of purpose transaction ID4 was generated, and a different value is written in by the case where it is generated by the personal computer 50 the case where transaction ID is generated by the distributing server 10 for management of distribution, and for local use. When transaction ID is generated for local use that is, with the personal computer 50. When transaction ID is generated locally because of ripping or check-in, "0" is written in the fixation flag 7 of the fixed area 6, and when transaction ID is generated for the purpose of distribution, "1" is written in the fixation flag 7 of the fixed area 6. Transaction ID is generated by generating of a random number.
[0365]A license key is a common key in the Triple-DES method by 2key at the time of license generating, is used for a contents data encryption and decoding, and is generated by generating of a random number.
[0366]With reference to drawing 37, the access control information ACm comprises number-of-times Play_count of refreshable, and movement and copy-control-information Move_count. 1 byte is assigned to number-of-times Play_count of refreshable, movement and copy-control-information Move_count, and protecting level Safe_Level, respectively.
[0367]Either ""0" which shows the reproduction failure of enciphered content data, "1-254" which show the number of times of refreshable of enciphered content data and 255" which shows that enciphered content data is indefinitely renewable is written in number-of-times Play_count of refreshable. When the number of times "1-254" of refreshable is written in, whenever enciphered content data is reproduced, the number of times of refreshable is reduced every [1].
[0368]In movement and copy-control-information Move_count. "0" which shows that movement and the duplicate of enciphered content data and a license are forbidden, movement of enciphered content data and a license being impossible, and, "1-15" which show that the duplicate of enciphered content data and a license is permitted with restriction, Movement of enciphered content data and a license is permitted with restriction, And "240-253" which show that the duplicate of enciphered content data and a license is improper, movement of enciphered content data and a license being permitted, and, Either of "255" which shows that movement and the duplicate of "254" and enciphered content data in which it is shown that the duplicate of enciphered content data and a license is forbidden, and a license are permitted indefinitely is written in. When "1-15" are written in movement and copy-control-information Move_count, whenever enciphered content data and a license are reproduced, a numerical value is reduced every [1]. And when a numerical value is set to "0", movement and the duplicate of enciphered content data and a license are forbidden. When "240-253" are written in movement and copy-control-information Move_count, whenever enciphered content data and a license are moved, a numerical value is increased by every [1]. And when a numerical value amounts to 254, movement of enciphered content data and a license is permitted, and the duplicate of enciphered content data and a license is forbidden. "17-239" are intact.
[0369]Protecting level Safe_Level evaluates the security level needed for a license. It has arranged so that it can respond, when the length of the key used for cipher processing, the security intensity which records a license, etc. are changed in the future. For example, rather than it secures security and protecting contents by software using a program like the license management module mentioned above like MEMOKADO 110 or the contents playback device 1550, By hardware, secure security and protect [that a security level will be / way / high] contents.
[0370]The reproduction control information ACp consists of 1 byte of flag, and two or

more information which serves as hand validity by flag. flag(i) shows eye i bit of 1 byte of flag. And the reproduction control information ACp comprises flag(0) flag(1) flag(2)+Play_length, flag(3)+not_after, flag(4) not_before, and flag(5)+Region_code.
[0371]flag (0) ** propriety of conversion of the reproduction speed of enciphered content data. flag (1) shows the propriety of edit of enciphered content data. flag(2)+Play_length shows the size of the partial regeneration, when showing and carrying out partial regeneration of the refreshable size of enciphered content data. flag(3)+not_after shows the time which use of enciphered content data ends. flag(4) not_before shows the time which can start use of enciphered content data. flag(5)+Region_code shows the area code of enciphered content data. Use of the enciphered content data in flag(3)+not_after and flag(4) not_before means reproduction of enciphered content data, movement, a duplicate, check-out, and check-in.
[0372]Either of "0" which forbids check-out, and "one or more numbers" which show the number of times which can be checked out is written in number checkout_count which can be checked out. And whenever it is checked out, a numerical value is reduced every [1], and when "one or more numbers" is written in number checkout_count which can be checked out, whenever he checks in, a numerical value is increased by every [1].
[0373]The license generating means 5403 generates a license and number checkout_count which can be checked out at the time of ripping from the content ID, transaction ID, the license key, the access restriction information ACm, and the reproduction control information ACp of the contents mentioned above.
[0374]The enciphered content data and the license which were acquired from the audio CD by ripping are managed by software like the enciphered content data and the license which were received with the license management module 511.
[0375]In the above, although the personal computer 50 acquired enciphered content data and a license from the audio CD by ripping, In this invention, ripping may generate enciphered content data and a license from the contents data received not only by this but by the internet delivery. Although the personal computer 50 receives enciphered content data and a license, exchanging a public key, a common key, etc. between the distributing servers 10 using Internet network 30 shown in drawing 1 and drawing 2, and performing mutual recognition, When acquiring enciphered content data and a license by ripping, the usual internet delivery receives contents data, without performing an exchange of such a public key and a common key.
[0376]Therefore, the personal computer 50, When the usual Internet is not accessed, When enciphered content data and a license can be acquired from an audio CD by ripping and the usual Internet is accessed, Enciphered content data and a license are acquirable from the contents data distributed by the Internet by ripping. Therefore, the Internet does not necessarily need to be accessed and what is necessary is just to build in a CD-ROM drive in this invention, in order for the personal computer 50 to acquire enciphered content data and a license. And when acquiring enciphered content data and a license by ripping, a personal computer, It is necessary to build in neither the license management device 520 nor the license management module 511, and what is necessary is just to build in the software performed by each means of the functional block diagram shown in drawing 33.
[0377]Of course, the personal computer by this invention, It may have a function in which the license management device 520 and the license management module 511 other than the function which acquires enciphered content data and a license by ripping receive enciphered content data and a license.
[0378]Since the license by ripping is generated by the personal computer 50, the license is called "local license."

[0379]According to the embodiment of the invention, a personal computer, Contents data is acquired from an audio CD by an internet delivery, Since enciphered content data and a license are generated according to the contents of the watermark (it is also called duplicate propriety information.) contained in the contents data, Generation of the enciphered content [ripping] data according to the contents of the watermark and a local license is possible.

[0380]With all the points, the embodiment indicated this time is illustration and should be considered not to be restrictive. The range of this invention is shown by the above-mentioned not explanation but claim of an embodiment, and it is meant that all the change in a claim, an equivalent meaning, and within the limits is included.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a schematic diagram which illustrates a data distribution system notionally.

[Drawing 2]It is a schematic diagram which illustrates other data distribution systems notionally.

[Drawing 3]It is a figure showing the characteristics, such as data for the communication in the data distribution system shown in drawing 1 and drawing 2, and information.

[Drawing 4]It is a figure showing the characteristics, such as data for the communication in the data distribution system shown in drawing 1 and drawing 2, and information.

[Drawing 5]It is a schematic block diagram showing the composition of the distributing server in the data distribution system shown in drawing 1 and drawing 2.

[Drawing 6]It is a schematic block diagram showing the composition of the personal computer in the data distribution system shown in drawing 1 and drawing 2.

[Drawing 7]It is a schematic block diagram showing the composition of the portable telephone in the data distribution system shown in drawing 2.

[Drawing 8]It is a schematic block diagram showing the composition of the memory card in the data distribution system shown in drawing 1 and drawing 2.

[Drawing 9]It is a schematic block diagram showing the composition of the license management device built in the personal computer shown in drawing 6.

[Drawing 10]It is the 1st flow chart for explaining high distribution operation of the security level in the data distribution system shown in drawing 1 and drawing 2.

[Drawing 11]It is the 2nd flow chart for explaining high distribution operation of the security level in the data distribution system shown in drawing 1 and drawing 2.

[Drawing 12]It is the 3rd flow chart for explaining high distribution operation of the security level in the data distribution system shown in drawing 1 and drawing 2.

[Drawing 13]It is the 4th flow chart for explaining high distribution operation of the security level in the data distribution system shown in drawing 1 and drawing 2.

[Drawing 14]It is the 1st flow chart for explaining low distribution operation of the security level in the data distribution system shown in drawing 1 and drawing 2.

[Drawing 15]It is the 2nd flow chart for explaining low distribution operation of the security level in the data distribution system shown in drawing 1 and drawing 2.

[Drawing 16]It is the 3rd flow chart for explaining low distribution operation of the security level in the data distribution system shown in drawing 1 and drawing 2.

[Drawing 17]It is the 4th flow chart for explaining low distribution operation of the security level in the data distribution system shown in drawing 1 and drawing 2.

[Drawing 18]It is the 1st flow chart for explaining the moving operation of a license of the enciphered content data in the data distribution system shown in drawing 1 and drawing 2.
[Drawing 19]It is the 2nd flow chart for explaining the moving operation of a license of the enciphered content data in the data distribution system shown in drawing 1 and drawing 2.
[Drawing 20]It is the 3rd flow chart for explaining the moving operation of a license of the enciphered content data in the data distribution system shown in drawing 1 and drawing 2.
[Drawing 21]It is the 4th flow chart for explaining the moving operation of a license of the enciphered content data in the data distribution system shown in drawing 1 and drawing 2.
[Drawing 22]It is the 1st flow chart for explaining check-out operation of a license of the enciphered content data in the data distribution system shown in drawing 1 and drawing 2.
[Drawing 23]It is the 2nd flow chart for explaining check-out operation of a license of the enciphered content data in the data distribution system shown in drawing 1 and drawing 2.
[Drawing 24]It is the 3rd flow chart for explaining check-out operation of a license of the enciphered content data in the data distribution system shown in drawing 1 and drawing 2.
[Drawing 25]It is the 4th flow chart for explaining check-out operation of a license of the enciphered content data in the data distribution system shown in drawing 1 and drawing 2.
[Drawing 26]It is the 1st flow chart for explaining check-in operation of a license of the enciphered content data in the data distribution system shown in drawing 1 and drawing 2.
[Drawing 27]It is the 2nd flow chart for explaining check-in operation of a license of the enciphered content data in the data distribution system shown in drawing 1 and drawing 2.
[Drawing 28]It is the 3rd flow chart for explaining check-in operation of a license of the enciphered content data in the data distribution system shown in drawing 1 and drawing 2.
[Drawing 29]It is the 1st flow chart for explaining the reproduction motion in a portable telephone.
[Drawing 30]It is the 2nd flow chart for explaining the reproduction motion in a portable telephone.
[Drawing 31]It is a figure showing the composition of the contents list file in the hard disk of a personal computer.
[Drawing 32]It is a figure showing the composition of the reproduction list file in a memory card.
[Drawing 33]It is a functional block diagram for explaining the function of software to perform ripping.
[Drawing 34]It is a flow chart for explaining operation of ripping in the data distribution system shown in drawing 1 and drawing 2.
[Drawing 35]It is a format figure of content ID.
[Drawing 36]It is a format figure of transaction ID.
[Drawing 37]It is a chart of a ****** sake about the composition of media access conditions, a decoder access condition, and the number that can be checked out.
[Description of Notations]
1 Content ID, and 2 and 5 A fixed area, and 3 and 6 A management domain and 4

Transaction ID, 7MSB 8 reserve, 10 distributing servers, and 20 A distribution career, 30 Internet networks, 40 A modem and 50 A personal computer, 60 CD, 70 USB cables, 100,102 A portable telephone and 110 A memory card and 130 Head telephone, 150 A contents list file and 160 Reproduction list file, 302 A charge database, 304 information databases, a 306 CRL database, 307 A menu database and 308 A distribution recording data base, 310 data processing parts, 312,320,1404, 1408,1412,1422, 1504,1510,1516, 5204,5208,5212, and 5222 Decoding processing section, 313 An authentication key attaching part and 315 A distribution control part, 316, a session key generating part, 318, 326, 328, 1406, 1410, 1417, 1506, 5206, 5210, 5217, and 5405 A communication apparatus, and 510-1106, 1420 and 5220 A cipher-processing part and 350 A controller, a 511 license-management module, 520 A license management device and 530 A hard disk, 540 CD-ROM drives, 550-1112 USB interfaces and 560 A keyboard and 570 Display, 580-1114, 1426, 1530, and 5226 A terminal, 1108 navigational panels, 1110 A display panel and 1200 A memory card interface, 1400-1500, a 5200 authentication-data attaching part, A 1402-5202 Kmc attaching part, a 1414-5214 KPa attaching part, 1415-5215 A memory, a 1415 A-5215A CRL field, 1415B A regenerated list, a 1415 C-5215B license area, 1415D A data area, a 1416-5216 KPmc attaching part, and 1418-5218 Session key generating part, A 1421-5221 Km attaching part and 1424-5224 Interface, 1442-1446 change-over switches, 1502 Kpl attaching part, and 1518 Music reproduction section, 1519 A DA converter, a 1521-1525-1621-162n license management file, and 1531-1535-1611-161n A contents file, a 1550 contents-playback device, 5400 A watermark detection means and 5401 [Music encoder.] A watermark judging means and 5402 A remark means and 5403 A license generating means and 5404